About This Guide

This section discusses the objectives, audience, organization, and conventions of the *Cisco 2500 Series Access Server User Guide*.

All Cisco technical documentation and additional literature are available on UniverCD, Cisco's online library of product information. UniverCD is updated and shipped monthly, so it might be more up to date than printed documentation. UniverCD is available both as a single CD and as an annual subscription. To order UniverCD, contact your local sales representative or call Customer Service.

Document Objectives

This publication will step you through initial site preparation, installation, configuration and troubleshooting of the Cisco 2500 series access server. It also covers selected maintenance procedures, such as replacing single in-line memory modules (SIMMs) and Flash memory. The appendix "Internetworking Primer" has been included to provide the required background for getting started with your Cisco 2500 series access server.

Audience

This publication is designed for the person installing the access server, who should be familiar with electronic circuitry and wiring practices and have experience as an electronic or electromechanical technician.

For a tutorial on initial software configuration, refer to the appendix "Internetworking Primer," and the publication *Router Products Getting Started Guide*. For more advanced configuration applications, refer to the *Router Products Configuration Guide* and the *Router Products Command Reference*.

Document Organization

The major sections of this user guide are as follows:

- Chapter 1, “Overview of the Cisco 2500 Series Access Server,” discusses the features and specifications of the Cisco 2500 series access server.
- Chapter 2, “Preparing to Install the Cisco 2500 Series Access Server,” discusses environmental requirements and preparation for network connections, and describes the various ports and how to prepare for connections between networks and ports.
- Chapter 3, “Installing the Cisco 2500 Series Access Server,” includes cabling and basic installation information.
- Chapter 4, “Configuring the Cisco 2500 Series Access Server,” discusses configuration for the console and modems and other asynchronous devices attached to the Cisco 2500 series access servers using AutoInstall, manually using the automated setup utility, or manually without using the setup utility.
- Appendix A, “Internetworking Primer,” includes basic information on the Cisco IOS operating environment, LANs, WANs, desktop protocols, modems, and asynchronous protocols.
- Appendix B, “Maintaining the Cisco 2500 Series Access Server,” discusses maintenance procedures, including items such as Flash memory SIMM replacement, system code upgrades, and DRAM replacement.
- Appendix C, “Cable Specifications,” lists pinout information for all cables used with the Cisco 2500 series access server.
- Appendix D, “Translated Safety Warnings,” contains translations for the warnings that appear in this manual.

Document Conventions

This publication uses the following conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** font.
- Variables for which you supply values are in *italic* font.
- Elements in square brackets ([ ]) are optional.
- Alternative but required keywords are grouped in braces ({ }) and are separated by a vertical bar (|).

Examples use these conventions:

- Terminal sessions are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters are shown in angle brackets (< >).
- Information the system displays is in `screen` font, with default responses in square brackets ([ ]).

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Caution Means r*eader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. To see translated versions of this warning, refer to the appendix "Translated Safety Warnings."

CHAPTER 1

Overview of the Cisco 2500 Series Access Server

The Cisco 2500 series access server is a full-featured communication server with multiprotocol routing capability between synchronous serial, LAN, and asynchronous serial ports.

The Cisco 2500 series access server is available in four models, as follows:

Model 2509 1 Ethernet port
2 synchronous serial ports
8 asynchronous serial ports

Model 2510 1 Token Ring
2 synchronous serial ports
8 asynchronous serial ports

Model 2511 1 Ethernet
2 synchronous serial ports
16 asynchronous serial ports

Model 2512 1 Token Ring
2 synchronous serial ports
16 asynchronous serial ports

Access Server Hardware Features

The access server has the following hardware features:

- 8 or 16 ports for connection to modems, terminals, or other asynchronous (EIA/TIA-232) equipment
- 2 MB to 16 MB (depending on the selected feature set) of primary memory, using dynamic random-access memory (DRAM) single in-line memory modules (SIMMs)
- 32-KB nonvolatile random-access memory (NVRAM) to store configurations
- 4-MB to 8-MB Flash memory for running the Cisco Internetwork Operating System (Cisco IOS) image
- 2-MB shared packet memory
- Two synchronous serial ports for connection to a WAN
- EIA/TIA-232 console port for connection of a console terminal
- EIA/TIA-232 auxiliary port for connection of a terminal or modem

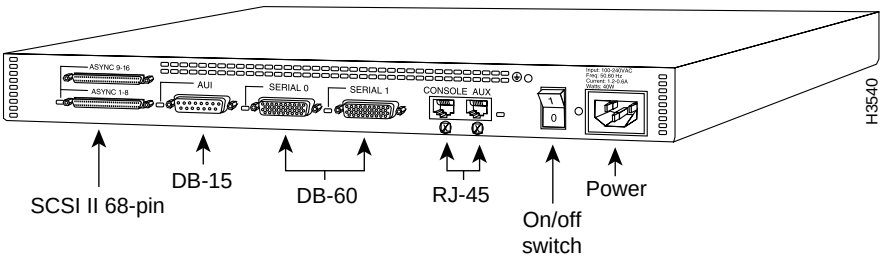
Note EIA/TIA-232 and EIA/TIA-449 were known as recommended standards RS-232 and RS-449 before their acceptance as standards by the Electronic Industries Association (EIA) and Telecommunications Industry Association (TIA).

The serial WAN connections use a proprietary, 60-pin connector. The Ethernet and Token Ring connections use standard LAN cabling with an attachment unit interface (AUI) or DB-9 connector.

The console terminal is used to provide basic and emergency local system access. The auxiliary port is used to provide basic and emergency remote system access.

The access server uses a 68-pin connector and breakout cable, which provides 8 RJ-45 ports on each cable. These ports use RJ-45-to-DB-25 adapters to connect to asynchronous devices.

Figure 1-1 Cisco 2500 Series Access Server (Model 2511 Shown)



Access Server Services

The access server connects terminals, printers, modems, microcomputers, and remote LANs over asynchronous serial lines to an internetwork. The access server uses a set of connection services to allow remote networks access to an internetwork of LANs and WANs.

The access server supports four types of server operation:

- Remote node services
- Terminal services
- Asynchronous routing services
- Protocol translation services

Remote Node Services

Remote node services support remote network connectivity with Serial Line Internet Protocol (SLIP), Point-to-point Protocol (PPP), AppleTalk Remote Access Protocol (ARA protocol), and XRemote.

Terminal Services

Terminal services provide terminal-to-host connectivity with virtual terminal protocols including Telnet, local-area transport (LAT), TN3270, and rlogin. Terminal services can be used to connect to a modem in a modem pool for outbound connectivity.

Asynchronous Routing Services

Routing services enable the access server to route packets over LANs and WANs using asynchronous interfaces to a remote LAN or WAN.

Protocol Translation Services

Protocol translation allows terminal services running over one protocol to be translated to terminal services running over another protocol such as an X.25 packet assembler/disassembler (PAD) to Telnet (using Transmission Control Protocol/Internet Protocol [TCP/IP]). Protocol translation on the access server supports Telnet, TN3270, LAT, X.25, and PAD.

System Specifications

The system specifications of the Cisco 2500 series access server are listed in Table 1-1.

Table 1-1 System Specifications

Description	Specification
Dimensions (H x W x D)	1.75 x 17.5 x 10.56" one rack unit (4.44 x 44.45 x 26.82 cm)
Weight	10 lb (4.5 kg)
Input voltage, AC power supply Current Frequency Power dissipation	100–240 VAC 0.5–1.0A 50–60 Hz 40W (maximum), 135.5 Btus[1]/hr

Description	Specification
Input voltage, DC power supply Current Power dissipation	40W, 40–72 VDC 0.5–1.0A 40W (maximum), 135.5 Btus/hr
Processor	20-MHz Motorola 68EC030
Network interface options	Model 2509:1 Ethernet, 2 synchronous serial, 8 asynchronous serial Model 2510: 1 Token Ring, 2 synchronous serial, 8 asynchronous serial Model 2511: 1 Ethernet, 2 synchronous serial, 16 asynchronous serial Model 2512: 1 Token Ring, 2 synchronous serial, 16 asynchronous serial
Ethernet interface	Ethernet AUI IEEE 802.3
Token Ring interface	IEEE 802.5 (DB-9)
Synchronous serial interfaces	EIA/TIA-232, EIA/TIA-449, V.35, X.21 (NRZ/NRZI[2] and DTE/DCE[3] mode) EIA-530 (NRZ/NRZI and DTE mode) All synchronous serial interfaces use the DB-60 connector at the chassis
Asynchronous serial interfaces	EIA/TIA-232, Asynchronous serial interfaces use RJ-45 connectors
Console and auxiliary ports	Asynchronous serial (RJ-45)
Operating environment	32–104°F (0–40°C)
Nonoperating temperature	–40–185°F (–40–85°C)
Operating humidity	5–95%, noncondensing
Noise level	34 dBa @ 3' (0.914 m)

1. BTU = British thermal unit.
2. NRZ = nonreturn to zero; NRZI = nonreturn to zero inverted.
3. DTE = data terminal equipment; DCE = data communications equipment.

CHAPTER 2

Preparing to Install the Cisco 2500 Series Access Server

This chapter describes the tasks you must perform before you begin to install the Cisco 2500 series access server. It includes the following sections:

- Safety Recommendations
- General Site Requirements
- Installation Checklist
- Creating a Site Log
- Cabling Considerations
- Console and Auxiliary Port Considerations
- Network Connection Considerations
- Inspecting the System

Safety Recommendations

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- Put the removed chassis cover in a safe place.
- Keep tools away from walk areas where you and others could fall over them.
- Do not wear loose clothing that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.

- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

Maintaining Safety with Electricity

Follow these guidelines when working on equipment powered by electricity.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or can weld the metal object to the terminals. (To see translated versions of this warning, refer to the appendix "Translated Safety Warnings.")

- Locate the emergency power-off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.
- Disconnect all power by turning off the power and unplugging the power cord before doing the following:
  - Installing or removing a chassis
  - Working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit. Always check.

Warning Read the installation instructions before you connect the system to its power source. (To see translated versions of this warning, refer to the appendix "Translated Safety Warnings.")

- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs, proceed as follows:
  - Use caution; do not become a victim yourself.
  - Turn off power to the system.
  - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim and then call for help.
  - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It occurs when electronic components are improperly handled and can result in complete or intermittent failures.

Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to safely channel unwanted ESD voltages to ground. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

Caution For safety, periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms.

General Site Requirements

This section describes the requirements your site must meet for safe installation and operation of your system. Ensure that your site is properly prepared before beginning installation.

The access server can be placed on a desktop or mounted in a rack or on a wall.

Site Environment

The location of individual chassis and the layout of your equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause system malfunctions and shutdowns, and can make system maintenance difficult.

When planning your site layout and equipment locations, keep in mind the precautions described in the next section, "Preventive Site Configuration" to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are currently experiencing shutdowns or unusually high errors with your existing equipment, these precautions may help you isolate the cause of failures and prevent future problems.

Preventive Site Configuration

The following precautions will help you plan an acceptable operating environment for your access server and will help you avoid environmentally caused equipment failures:

- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Ensure that the room in which you operate your system has adequate air circulation.
- Always follow the ESD-prevention procedures described in the section "Safety Recommendations" earlier in this chapter to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Ensure that the chassis cover is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which may interrupt and redirect the flow of cooling air from internal components.

Configuring Equipment Racks

The following tips will help you plan an acceptable equipment rack configuration:

- Enclosed racks must have adequate ventilation. Ensure that the rack is not overly congested because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.

- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or the exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack, which are found by experimenting with different arrangements.

Power Supply Considerations

Check the power at your site to ensure that you are receiving "clean" power (free of spikes and noise). Install a power conditioner if necessary.

Warning The device is designed to work with TN power systems. (To see translated versions of this warning, refer to the appendix "Translated Safety Warnings.")

The access server power supply includes the following features:

- Autoselects either 110V or 220V operation.
- All units include a 6-foot (1.8-meter) electrical power cord. (A label near the power cord indicates the correct voltage, frequency, current draw, and power dissipation for your unit.)

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors). (To see translated versions of this warning, refer to the appendix "Translated Safety Warnings.")

Installation Checklist

The Installation Checklist lists the procedures for initial hardware installation of a new access server. Make a copy of this checklist and mark the entries as you complete each procedure. Include a copy of the checklist for each system in your Site Log. (See the following section, “Creating a Site Log.”)

Installation checklist for site_____

Access server name_____

Task	Verified by	Date
Installation checklist copied		
Background information placed in Site Log		
Site power voltages verified		
Installation site prepower check completed		
Required tools available		
Additional equipment available		
Access server received		
Optional UniverCD received or ordered, printed documentation received		
Chassis components verified		
Initial electrical connections established		
ASCII terminal attached to console port, or modem attached to console port (for remote configuration)		
Signal distance limits verified		
Startup sequence steps completed		
Initial system operation verified		
Software image verified		

Creating a Site Log

The Site Log provides a record of all actions relevant to the system. Keep it near the chassis where anyone who performs tasks has access to it. Use the Installation Checklist (see the previous section "Installation Checklist") to verify steps in the installation and maintenance of your system. Site Log entries might include the following:

- Installation progress—Make a copy of the Installation Checklist and insert it into the Site Log. Make entries on the checklist as you complete each procedure.
- Upgrades and maintenance procedures—Use the Site Log as a record of ongoing system maintenance and expansion. Each time a procedure is performed on the system, update the Site Log to reflect the following:
  - Configuration changes
  - Changes and Updates to Cisco IOS software
  - Maintenance schedules and requirements
  - Corrective maintenance procedures performed
  - Intermittent problems
  - Related comments and notes

Cabling Considerations

When setting up your access server, consider distance limitations and potential electromagnetic interference (EMI) as defined by the Electronic Industries Association (EIA).

Warning The ports labeled "Ethernet," "10BaseT," "Token Ring," "Console," and "AUX" are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Because the BRI circuits are treated like telephone-network voltage, avoid connecting the SELV circuit to the telephone network voltage (TNV) circuits. (To see translated versions of this warning, refer to the appendix "Translated Safety Warnings.")

Distance Limitations

Following are the distance limitation specifications for Ethernet, Token Ring, and serial interfaces.

Ethernet Connections

The distance limitations for the IEEE 802.3 (10Base5 coaxial cable) specification indicate a maximum segment distance of 1,640 feet (500 m) at a transmission rate of 10 megabits per second (Mbps).

The distance limitations for Ethernet 10BaseT indicate a maximum segment distance of 328 feet (100 m); Ethernet 10Base2 has a maximum segment distance of 656 feet (200 m).

Token Ring Connections

The distance limitations for the IEEE 802.5 specification indicate a maximum segment distance of 328 feet (100 m) at a transmission rate of 4 or 16 Mbps for unshielded twisted-pair (UTP) cable. The distance limitation when using shielded twisted-pair (STP) cabling is 1,640 feet (500 m).

Serial Connections

As with all signaling systems, EIA/TIA-232 signals can travel a limited distance at any given bit rate; generally, the slower the data rate, the greater the distance. Table 2-1 shows the standard relationship between baud rate and maximum distance.

Table 2-1 EIA/TIA-232 Speed and Distance Limitations

Data Rate (Baud)	Distance (Feet)	Distance (Meters)
2400	200	60
4800	100	30
9600	50	15
19,200	50	15

Data Rate (Baud)	Distance (Feet)	Distance (Meters)
38,400	50	15
57,600	25	7.6
115,200	12	3.7

The use of balanced drivers allows EIA/TIA-449 signals to travel greater distances than the EIA/TIA-232 standard. Table 2-2 lists the standard relationship between baud rate and maximum distance for EIA/TIA-449 signals. These limits are also valid for V.35 and X.21.

Table 2-2 EIA/TIA-449 Speed and Distance Limitations

Data Rate (Baud)	Distance (Feet)	Distance (Meters)
2400	4,100	1,250
4800	2,050	625
9600	1,025	312
19200	513	156
38400	256	78
56000	102	31
T1	50	15

Caution The EIA/TIA-449 and V.35 interfaces support data rates up to 2.048 Mbps. Exceeding this maximum could result in loss of data and is not recommended.

Console and Auxiliary Port Considerations

This section discusses important cabling information that must be considered before you connect the terminals or modems to console and auxiliary ports. The console port and the auxiliary port are used to provide access to the system either locally or remotely.

Console Port Connections

Each access server system includes an EIA/TIA-232 (RJ-45) console asynchronous serial port. This port connects to a terminal using an RJ-45 cable and an RJ-45-to-DB-25 adapter. Depending on the cable and the adapter used, this port will appear as a data terminal equipment (DTE) or data communications equipment (DCE) device at the end of the cable. To connect to a console terminal, use an RJ-45 rollover cable with a female DTE connector (labeled "Terminal") for connection to the console port. For detailed information on installing the console terminal see the section "Connecting to the Console Port" in the chapter "Installing the Cisco 2500 Series Access Server.")

The appendix "Cable Specifications" lists the pinout for the console port. The default parameters for the console port are 9600 baud, 8 data bits, no parity, and 2 stop bits. The console port does not support hardware flow control or modem control.

Auxiliary Port Connections

An EIA/TIA-232 (RJ-45) auxiliary asynchronous serial port is included on all access servers. This port can connect to a modem for remote maintenance, or terminal services. Use an RJ-45 rollover cable with a male modem (MMOD) adapter (labeled "Modem") for this connection. For detailed information on connecting devices to the auxiliary port, see the section "Connecting a Modem to the Auxiliary Port" in the chapter "Installing the Cisco 2500 Series Access Server." See the appendix "Cable Specifications" for the pinout for this auxiliary port.

Network Connection Considerations

This sections describes important cabling information that must be considered before making your network connections. The Ethernet or Token Ring ports are used to connect to a LAN; the synchronous serial ports are used to connect to a WAN; and the asynchronous ports are used to provide remote access to the access server.

Ethernet Connections

The Ethernet port is located on the left of the rear panel of the access server. The port is labeled AUI. Use an Ethernet transceiver to connect the access server directly to the network.

You can use the following equipment to connect to the Ethernet AUI port:

- An Ethernet AUI cable connected to a transceiver
- An Ethernet transceiver connected directly to the access server's AUI port

The connection to the AUI port can be attached using one of two connector types, as follows:

- Slide latch connectors
- Jackscrew connectors

Note Ethernet cables are not shipped as standard with the access server.

Token Ring Connections

The Token Ring port is located on the left of the rear panel and is labeled TOKEN RING. Use a standard 9-pin Token Ring lobe cable (not supplied) to connect the access server directly to a media attachment unit (MAU).

Synchronous Serial Connections

The synchronous serial interface ports are located on the rear of the access server to the right of the Ethernet or Token Ring connector. The ports are labeled SERIAL 0 and SERIAL 1 (from left to right when facing the rear panel). The serial ports are 60-pin, D-type connectors. All serial interfaces (except the EIA-530) can be configured as DTE or DCE, depending on the attached cable. All DTE serial ports require that external clocking be provided by a channel service unit/data service unit (CSU/DSU) or other DCE device.

You must use a special serial cable to connect the access server to a modem or CSU/DSU. This cable is available from Cisco and is usually ordered with the system. The cable uses a DB-60 connector on the chassis end. See the appendix "Cable Specifications" for cable pinouts. For ordering information, contact a customer service representative.

Note Because of the small size of the pins on the DB-60 serial connector, attempting to manufacture your own serial cables is not recommended.

Asynchronous Serial Connections

The asynchronous serial ports use one or two 68-pin connectors located on the far left of the rear panel. Each of the connectors provides eight asynchronous ports. The lower port is labeled ASYNC 1–8, and the upper port is labeled ASYNC 9–16. Breakout cables that divide into eight RJ-45 connectors each are connected to the asynchronous connectors.

RJ-45-to-DB-25 adapters are used to connect to external devices such as modems, printers, or terminals. RJ-45-to-DB-25 adapters are available from Cisco for either DCE or DTE connections. See the appendix “Cable Specifications” to select the correct adapter, and for pinouts for the RJ-45-to-DB-25 adapters.

Inspecting the System

Do not unpack the access server until you are ready to install it. If the final installation site will not be ready for some time, keep the chassis in its shipping container to prevent accidental damage. When you have determined where you want the access server installed, proceed with the unpacking.

The access server, cables, UniverCD or printed publications, and any optional equipment you ordered might be shipped in more than one container. When you unpack each shipping container, check the packing list to ensure that you received all of the following items:

- Access server
- 6-foot (1.8-meter) power cord
- Jackscrews for the AUI connector
- Console and auxiliary cabling kit (two RJ-45 roll-over cables, one terminal adapter, and one modem adapter)
- Optional equipment (such as network interface cables, and asynchronous breakout cables)

- Warranty pack
- UniverCD and optional printed publications, as specified on your order

Inspect all items for shipping damage. If anything appears to be damaged, or if you encounter problems when installing or configuring your system, contact a customer service representative.

CHAPTER 3

Installing the Cisco 2500 Series Access Server

This chapter guides you through the installation of the Cisco 2500 series access server and includes the following sections:

- Required Tools and Parts
- Installing the Rubber Feet
- Rack-Mounting the Chassis
- Wall-Mounting the Chassis
- Connecting to the Network
- Connecting the Console Terminal and Modem
- What to Do after Installing the Access Server Hardware

Caution If you plan to place the access server on a desk or table, do not place anything on top of the access server that weighs in excess of 10 pounds (4.5 kg). Excessive weight on top could damage the chassis.

Required Tools and Parts

Following are the tools and parts required to install the access server:

- Flat-blade screwdrivers: small, 3/16-inch (0.476 cm), and medium, 1/4-inch (0.625 cm)
- ESD-preventive wrist strap
- A thread-forming screw (not included), to attach a ground wire to the protective grounding terminal on the chassis rear panel
- Rubber feet for desktop installation.
- Rack-mount brackets (used for rack-mounting or wall-mounting) and hardware (optional), including screws you must provide for rack-mounting and wall-mounting.
- An interface cable for each interface you will connect.

In addition, you might need the following external equipment:

- Channel service unit/digital service unit (CSU/DSU) for the serial interfaces.
- Ethernet transceiver or Token Ring media attachment unit (MAU).
- Console terminal (an ASCII terminal or a PC running terminal emulation software) configured for 9600 baud, 8 data bits, no parity, and 2 stop bits. A terminal is required unless you are using the AutoInstall procedure. See the section “Connecting the Console Terminal and Modem” later in this chapter for the procedure to connect a console terminal.
- Modem for remote system access (optional).

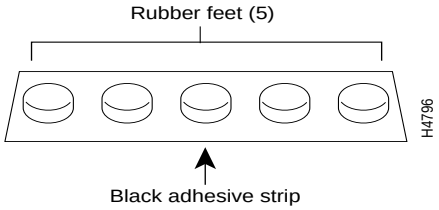
Installing the Rubber Feet

This section explains how to install the rubber feet on the bottom of the chassis. If you want to rack-mount the chassis, skip this section and proceed with the next section, "Rack-Mounting the Chassis." To wall-mount the chassis, skip this section and proceed with the section "Wall-Mounting the Chassis" later in this chapter.

Before placing the access server on a desktop, shelf, or other flat, secure surface, perform the following steps to install the rubber feet:

Step 1 Locate the rubber feet on the black adhesive strip that shipped with the chassis. (See Figure 3-1.)

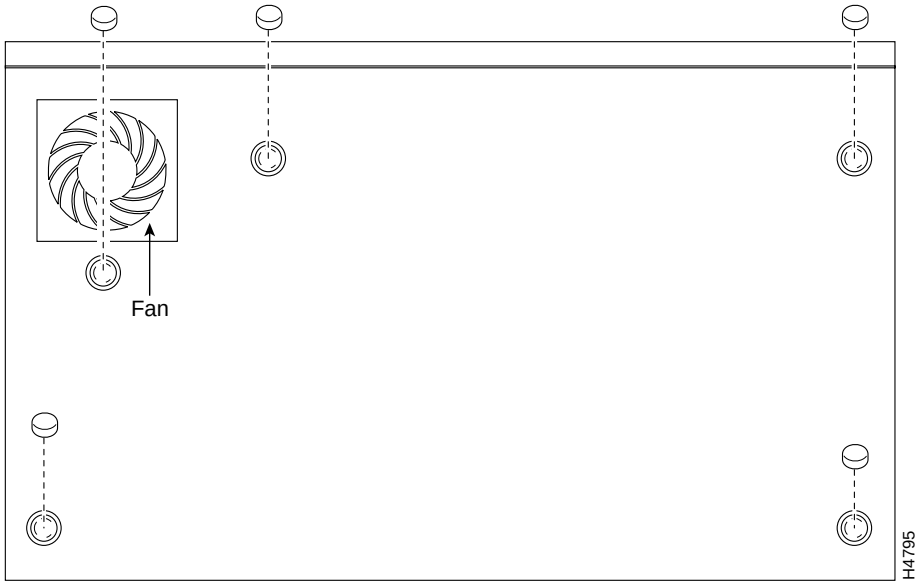
Figure 3-1 Identifying the Rubber Feet



Step 2 Place the access server upside down on a smooth, flat surface.

Step 3 Peel off one of the rubber feet from the black adhesive strip and place it adhesive-side down onto one of the five round recessed areas on the back of the chassis, as shown in Figure 3-2. Repeat this step to install the remaining four feet.

Figure 3-2 Installing the Rubber Feet



Rack-Mounting the Chassis

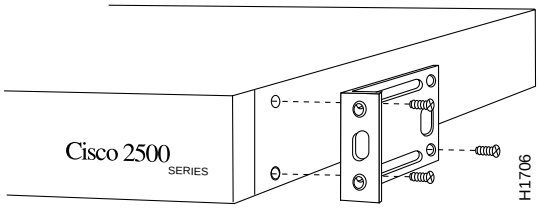
Depending on the rack you are using, attach the rack-mount brackets to the chassis using one of the following figures as a guide:

- Figure 3-3 and Figure 3-4 for 19-inch racks
- Figure 3-5 for 19-inch center-mount telco racks
- Figure 3-6 for installing the chassis in a rack (all rack types)

19-Inch Rack

To install the chassis in a 19-inch rack with the front panel forward, attach the rack-mount brackets as shown in Figure 3-3.

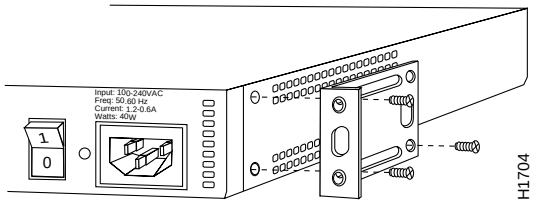
Figure 3-3 19-Inch Rack Installation—Front Panel Forward



Note: The second bracket attaches to the other side of the chassis.

To install the chassis in a 19-inch rack with the rear panel forward, attach the rack-mount brackets as shown in Figure 3-4.

Figure 3-4 19-Inch Rack Installation—Rear Panel Forward

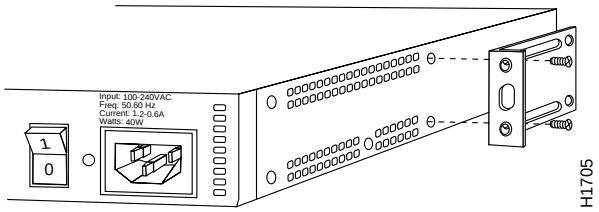


Note: The second bracket attaches to the other side of the chassis.

Telco Rack

To install the chassis in a 19-inch, center-mount telco rack, attach the rack-mount brackets as shown in Figure 3-5.

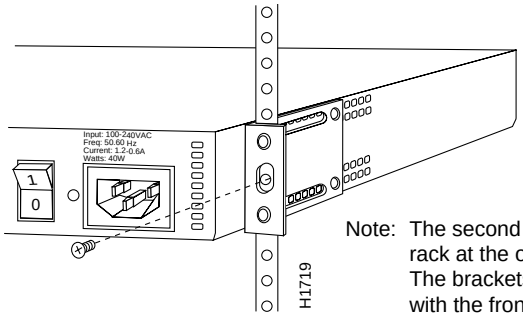
Figure 3-5 Telco Rack Installation—Rear Panel Forward



Note: The second bracket attaches to the other side of the chassis. The brackets can also be installed with the front panel forward.

Using the screws you provide, attach the chassis assemblies to the rack as shown in Figure 3-6.

Figure 3-6 Attaching the Chassis to the Rack—Rear Panel Forward



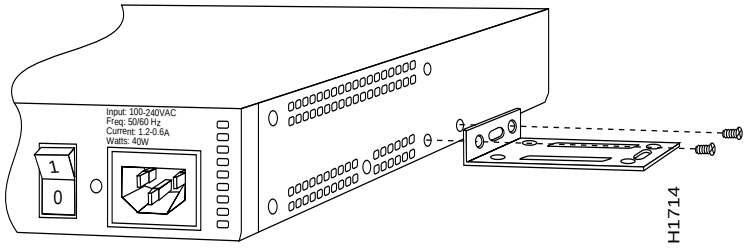
Note: The second bracket attaches to the rack at the other side of the chassis. The brackets can also be installed with the front panel forward.

Wall-Mounting the Chassis

Following is the procedure for wall-mounting the chassis:

Step 1 Attach the brackets as shown in Figure 3-7.

Figure 3-7 Attaching the Wall-Mount Brackets

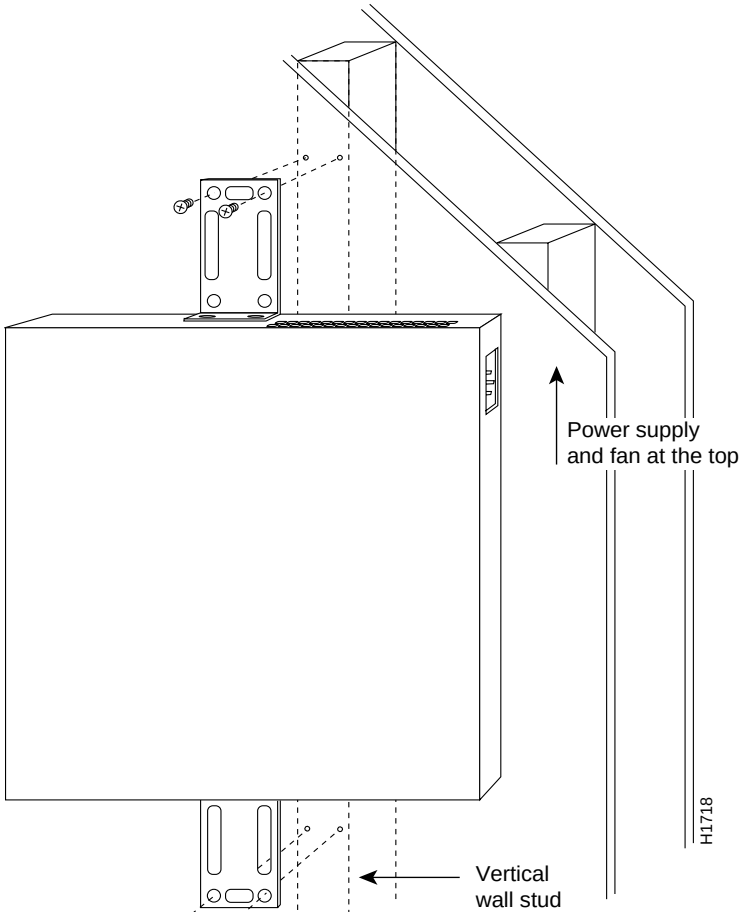


Step 2 Using screws and anchors you provide, attach the chassis assembly to the wall as shown in Figure 3-8. We recommend the following:

- For the best support of the chassis and cables, attach the brackets so that the screws align with a vertical wall stud.
- For the best ventilation of the chassis, mount the chassis with the power supply and fan at the top.

Caution To prevent the chassis from pulling away from the wall when cables are attached, align the brackets and screws with a vertical wall stud. (See Figure 3-8.) To ensure adequate ventilation, make sure there is clearance between the access server and the wall by adjusting the brackets on the access server. Mount the access server as shown in Figure 3-8, placing the chassis fan and power supply at the top.

Figure 3-8 Wall-Mounting the Chassis



Connecting to the Network

Take the following steps to connect the access server to your networks:

Note Refer to the document *Cisco 2500 Series Public Network Certification* for information on connection prerequisites and related warnings.

Step 1 Connect the Ethernet or Token Ring port to the transceiver or MAU as shown in Figure 3-9 or Figure 3-10.

Note If your Ethernet connection requires jackscrews, remove the slide-latch assembly from the AUI connector and attach the jackscrews provided.

Figure 3-9 Connecting Ethernet Transition Cables

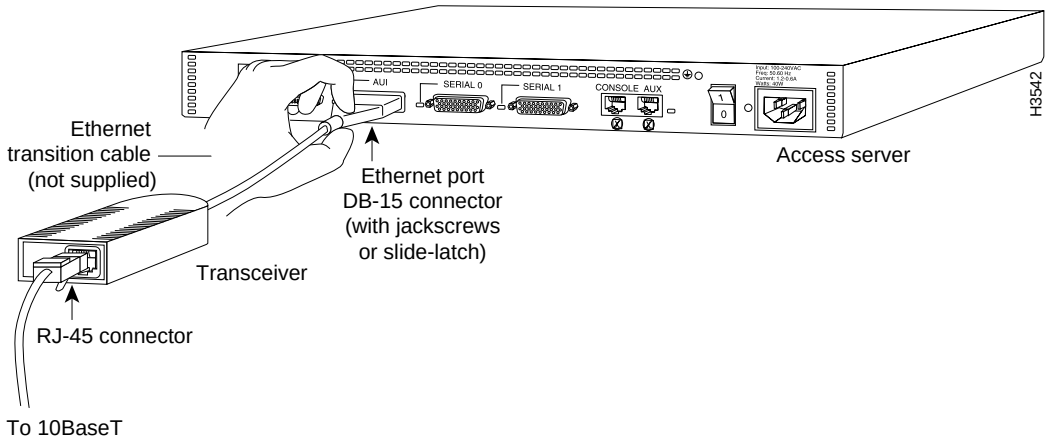
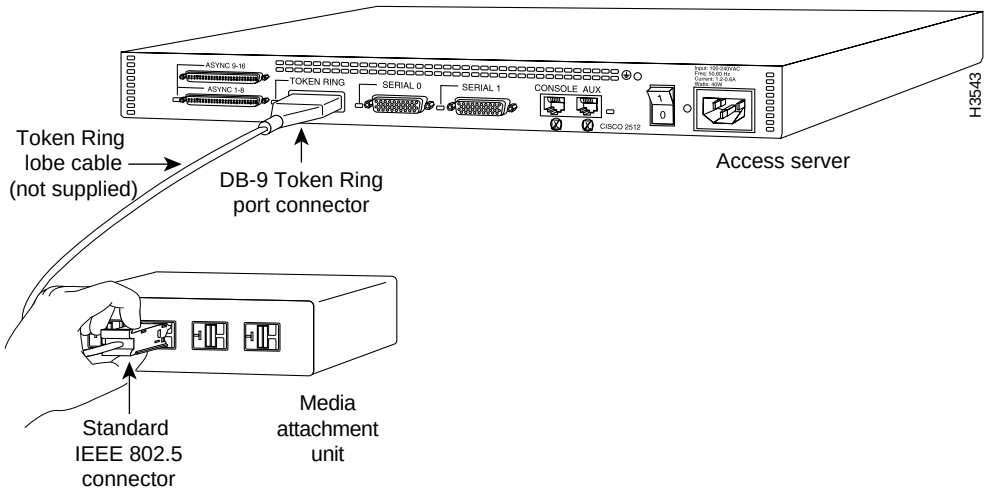
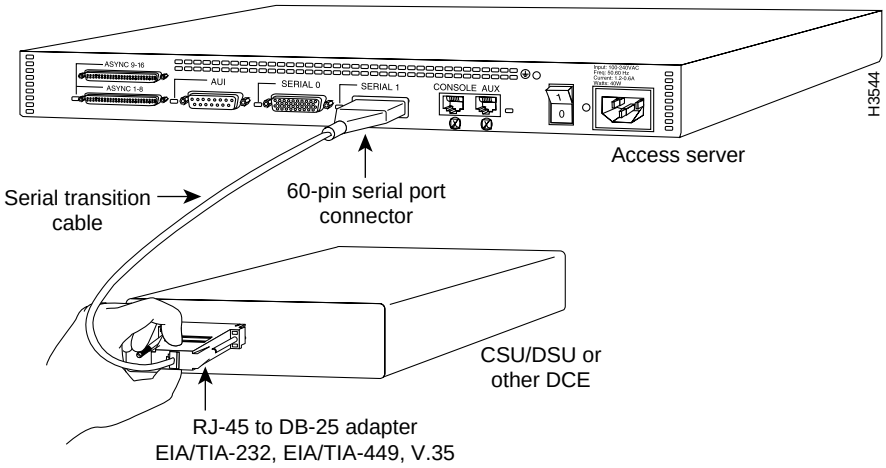


Figure 3-10 Connecting Token Ring Cables



Step 2 Connect the synchronous serial ports to the modem or CSU/DSU, as shown in Figure 3-11. Make certain to connect the 60-pin serial port connector as shown.

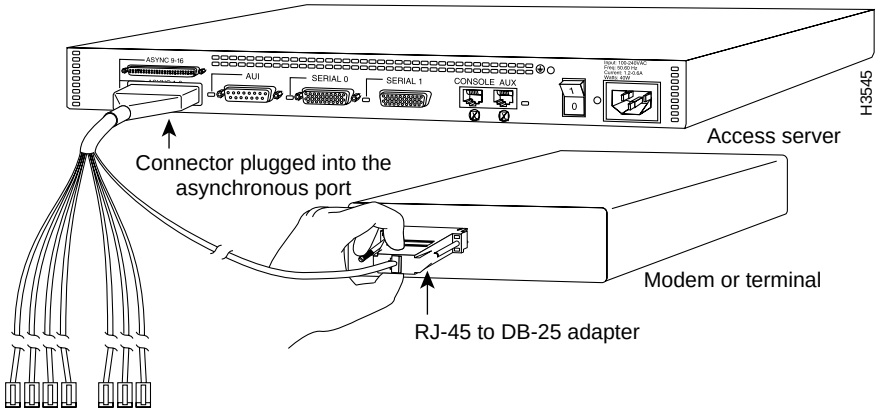
Figure 3-11 Connecting Synchronous Serial Cables



Step 3 Connect the asynchronous breakout cable to one of the 68-pin ports, and then use the RJ-45-to-DB-25 adapters to connect the breakout cable and your asynchronous devices. (See Figure 3-12.)

For additional instructions on connecting asynchronous devices to the breakout cable, refer to the appendix "Cable Specifications."

Figure 3-12 Connecting Asynchronous Serial Cables



Caution Make sure that the 68-pin connector on the breakout cable is securely connected to the access server. A short could occur which might damage the access server if the connection is disconnected.

Step 4 Using an M 3.5 thread-forming screw (not included), attach a ground wire to the protective grounding terminal on the rear panel of the chassis, as required by your installation.

Step 5 Connect the power cable between the access server and the AC source.

Connecting the Console Terminal and Modem

The console terminal is used to provide local administrative access to the access server. Connect the terminal to the console port. The auxiliary port can be used for with a terminal, or with a modem for remote access.

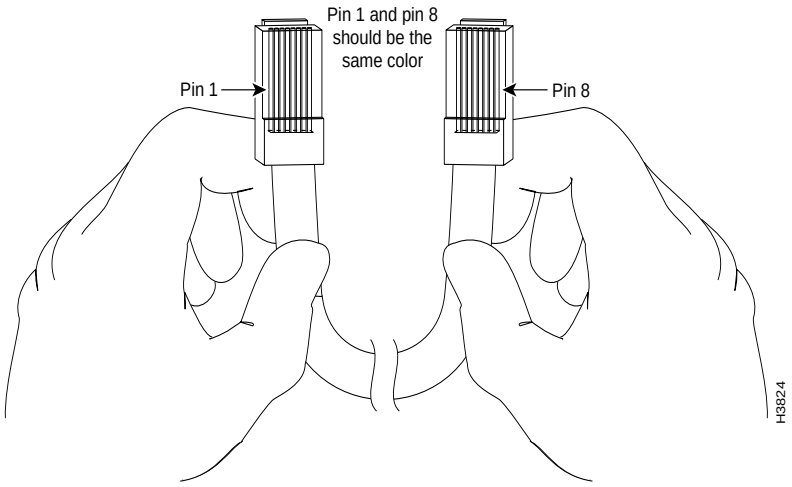
Connecting to the Console Port

This section explains how to connect a terminal (an ASCII terminal, or a PC running terminal emulation software) to the console port on the access server:

Step 1 Connect a terminal to the console port using a roll-over RJ-45 cable and an RJ-45-to-DB-25 adapter. If you are using the cable provided by Cisco, the adapter will be labeled “Terminal.”

A roll-over cable can be detected by comparing the two modular ends of the cable. Holding the cables in your hand, side-by-side, with the tab at the back, the wire connected to the pin on the outside of the left plug should be the same color as the pin on the outside of the right plug. (See Figure 3-13.) If your cable was purchased from Cisco, pin 1 will be white on one connector, and pin 8 will be white on the other (a rollover cable reverses pins 1 and 8, 2 and 7, 3 and 6, and 4 and 5).

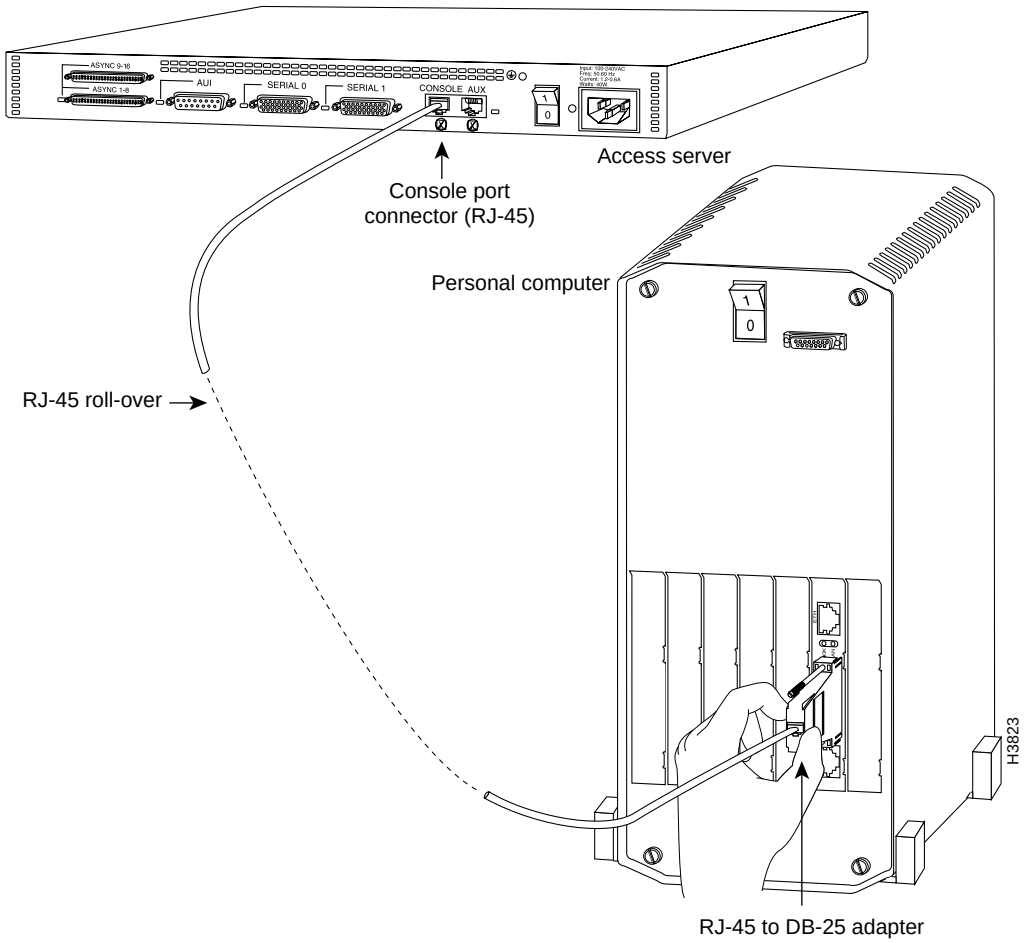
Figure 3-13 Identifying a Roll-Over Cable



Additional information on roll-over cable pinouts is available in the appendix "Cable Specifications."

Connection to a terminal will require an RJ-45-to-DB-25 adapter, and possibly a DB-25-to-DB9 adapter. (See Figure 3-14.)

Figure 3-14 Connecting the Console Terminal



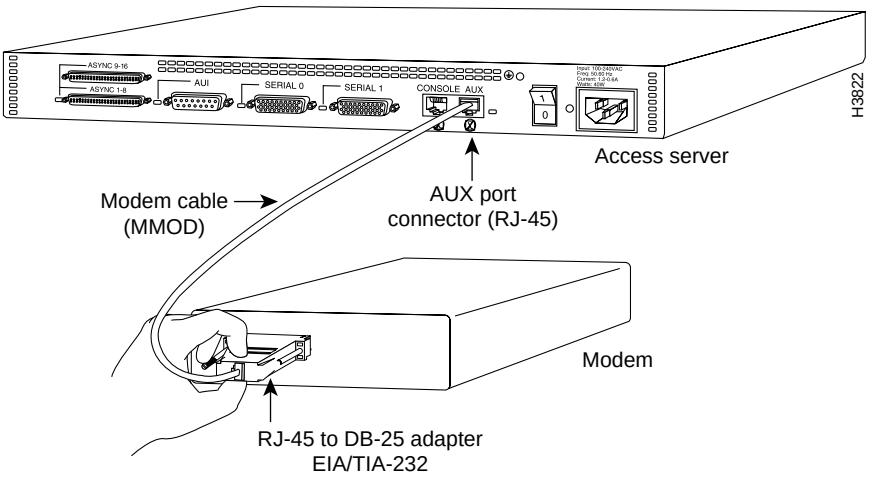
Step 2 Your terminal or PC terminal emulation software should be configured for 9600 baud, 8 data bits, no parity, and 2 stop bits (9600, 8/N/2).

Connecting a Modem to the Auxiliary Port

This section explains how to connect a modem to the console port on the access server:

Step 1 Connect a modem to the auxiliary port using a roll-over RJ-45 cable with an RJ-45-to-DB-25 adapter. The adapter provided by Cisco will be labeled "Modem." (See Figure 3-15.)

Figure 3-15 Connecting a Modem to the Auxiliary Port



Step 2 To configure the auxiliary port for modem operation, see the section "Modems" in the appendix "Internetworking Primer." Make sure that the modems and the auxiliary port are configured for the same transmission speed (38400 baud is normal) and hardware flow control with standard DCD and DTR operations.

What to Do after Installing the Access Server Hardware

After you install the access server hardware, the system is ready to be powered on and configured. For information on software configuration, refer to the chapter "Configuring the Cisco 2500 Series Access Server."

CHAPTER 4

Configuring the Cisco 2500 Series Access Server

This chapter describes the procedures for configuring the Cisco 2500 series access server and contains the following sections:

- Booting the Access Server for the First Time
- Using the Enable Secret and the Enable Password
- Configuring the Access Server

To configure your console, you need to connect a terminal to the access server. Configuration requires access to the console port.

If You Need More Information

The Cisco IOS software running the access server contains extensive features and functionality. The effective use of many of many of these features is easier if you have more information at hand. We recommend to you the following resources:

- UniverCD
- Cisco Information Online (CIO)
- Technical Assistance Center (TAC)

Additional Publications

For more information on configuring the Cisco 2500 series access server, see the appendix "Internetworking Primer," or refer to the following publications:

- *Access and Communication Servers Configuration Guide*
- *Access and Communication Servers Command Reference*
- *Configuration Builder Getting Started Guide*
- *Router Products Getting Started Guide*
- *Router Products Configuration Guide*
- *Router Products Command Reference*
- *Troubleshooting Internetworking Systems*

These publications are available on UniverCD.

All Cisco technical documentation and additional literature are available on UniverCD, Cisco's online library of product information. UniverCD is updated and shipped monthly, so it might be more up to date than printed documentation. UniverCD is available both as a single CD and as an annual subscription. To order UniverCD, contact your local sales representative or call Customer Service.

Contacting Customer Service

To obtain general information about Cisco Systems, Cisco's products or documentation, or upgrades, call 800 553-6387 or 408 526-7208. Customer Service hours are 5:00 a.m. to 6:00 p.m. Pacific time, Monday through Friday (excluding company holidays). You can also send e-mail to `cs-rep@cisco.com`.

Using Cisco Information Online

Cisco Information Online (CIO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CIO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CIO provides a wealth of standard and value-added services to Cisco's customers and business partners. CIO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CIO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CIO (called "CIO Classic") supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CIO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CIO in the following ways:

- WWW: `http://www.cisco.com`.
- Telnet: `cio.cisco.com`.
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CIO's Frequently Asked Questions (FAQ), contact `cio-help@cisco.com`. For additional information, contact `cio-team@cisco.com`.

Contacting the Technical Assistance Center

If you are a system administrator and need personal technical assistance with a Cisco product which is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447 or 408 526-7209, or send an e-mail message to `tac@cisco.com`. Emergency technical assistance (for network-down or severe network problems) is available 24 hours a day, 7 days a week.

When you contact the TAC for help, have the following information ready:

- Chassis serial number
- Maintenance contract number

- Software version level and hardware configuration (enter the **show version** command to display this information)
- Software configuration (enter the **show running config** (Release 11.0 or later) or the **write terminal** command (Earlier than Release 11.0) to display this information)

Contacting the European Technical Assistance Center

Cisco and its European Service Partners coordinate all customer service in Europe, including hardware and software telephone technical support, onsite service, and module exchange and repair. For more information, contact the European TAC.

European TAC numbers and e-mail address are as follows:

- Phone: 32 2 778 42 42
- Fax: 32 2 778 43 00
- E-mail: `euro-tac@cisco.com`

Booting the Access Server for the First Time

The access server is administered using the Cisco command interpreter, called the EXEC. You must log in to the access server before you can enter an EXEC command. For security purposes the EXEC has two levels of access to commands, user EXEC mode and privileged EXEC mode.

To enter the privileged mode you must enter the enable secret password on systems running Cisco Internetwork Operating System (Cisco IOS) Release 10.2(3) or later, or the enable password on systems running Cisco IOS releases prior to 10.2(3) or when using the boot ROM monitor.

Using the Enable Secret and the Enable Password

The commands available at the user level are a subset of those available at the privileged level. Because many privileged-level EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use.

There are two commands you can use to do this, depending on the release you have of the Cisco IOS software:

- **enable secret** *password* (which is a very secure, encrypted password).
- **enable** *password* (which is a less secure, or nonencrypted, password).

The enable secret password is available in Cisco IOS Release 10.2(3) or later. The **e**nable secret password is not available before Release 10.2(3). The enable password is available in all releases. You must enter the correct password to gain access to privileged-level commands.

On systems running Release 10.2(3) or later, the enable secret password is used. when you are running from the boot ROM, the enable password might be used depending on your ROM level.

The passwords should be different for maximum security. If you enter the same password for both during the setup script, the system will accept it, but you will receive a warning message indicating that you should enter a different password.

An enable secret password can contain from 1 to 25 uppercase and lowercase alphanumeric characters; an enable password can contain any number of uppercase and lowercase alphanumeric characters. In both cases, a number cannot be the first character. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored; trailing spaces are recognized.

If you lose or forget your enable password, see the section “Recovering a Lost Enable Password” in the chapter “Maintaining the Cisco 2500 Series Access Server.”

Configuring the Access Server

You can configure the access server following one of the procedures described in the following sections:

- Configuring the Access Server Using the Configuration Mode
- Configuring the Access Server Using AutoInstall
- Configuring the Access Server Manually Using the Setup Facility

Follow the procedure that best fits the needs of your network configuration.

Note You will need to acquire the correct network addresses from your system administrator or consult your network plan to determine correct addresses before you can complete the access server configuration. For details on network addressing, see the appendix "Internetworking Primer."

Before continuing the configuration process, check the current state of the access server by entering the **show version** command. The **show version** command will display the release of Cisco IOS software that is available on the access server.

Configuring the Access Server Using the Configuration Mode

You can configure the access server manually if you prefer not to use the setup facility or AutoInstall. Take the following steps to configure the access server manually:

Step 1 Connect a console terminal by following the instructions described in the section "Connecting the Console Terminal and Modem" in the chapter "Installing the Cisco 2500 Series Access Server" and then power up the access server.

Step 2 When you are asked if you would like to enter the initial dialog, answer **no** to go into the normal operating mode of the access server:

```
Would you like to enter the initial dialog? [yes]: no
```

Step 3 After a few seconds you will see the user EXEC prompt (Router>). Type **enable** to enter enable mode. Configuration changes can only be made in enable mode:

```
Router> enable
```

The prompt will change to the privileged EXEC prompt:

```
router#
```

Step 4 Enter the command **config terminal** at the enable prompt to enter configuration mode from the terminal:

```
router# config terminal
```

You can now enter any changes to the configuration that are desired. Press **Ctrl-Z** to exit configuration mode. (See the appendix "Internetworking Primer" for configuration assistance.)

To see the currently operating configuration, enter the command **show running-config** at the # prompt if you are running Cisco IOS Release 11.0 or later. Enter the command **write terminal** at the # prompt if you are running a Cisco IOS release earlier than 11.0:

```
router# show running-config
```

To see the configuration in NVRAM, enter the command **show startup-config** at the enable prompt.

```
router# show config
```

To make your changes permanent, enter the command **copy running-config startup-config** at the enable prompt if you are running Cisco IOS Release 11.0 or later. Enter the command **write memory** if you are running a Cisco IOS release earlier than 11.0:

```
router# copy running-config startup-config
********
```

The results of the **show running-config** and **show startup-config** commands will differ if you have made changes to the configuration, but have not yet written them to NVRAM.

The access server is now configured and will boot with the configuration you have entered.

Configuring the Access Server Using AutoInstall

The AutoInstall process is designed to configure the access server automatically after connection to your WAN. In order for AutoInstall to work properly, a Transmission Control Protocol/Internet Protocol (TCP/IP) host on your network must be preconfigured to provide the required configuration files. The TCP/IP host may exist anywhere on the network, as long as the following two conditions are maintained:

1. The host must be on the remote side of the access server's synchronous serial connection to the WAN.
2. User Datagram Protocol (UDP) broadcasts to and from the access server and the TCP/IP host must be enabled.

This functionality is coordinated by your system administrator at the site where the TCP/IP host is located. You should not attempt to use AutoInstall unless the required files have been provided on the TCP/IP host. See the publication *Access and Communication Server Configuration Guide* for information on how AutoInstall works.

Take the following steps to prepare your access server for the AutoInstall process:

Step 1 Attach the synchronous serial cable to the access server.

Step 2 Turn on power to the access server.

The access server will load the operating system image from Flash memory. If the remote end of the WAN connection is connected and properly configured, the AutoInstall process will begin.

If the AutoInstall completed successfully, you may wish to write the configuration data to the access server's nonvolatile random-access memory (NVRAM). Perform the following step to complete this task:

Step 3 At the # prompt, enter the **copy running-config startup-config** command if you are running Cisco IOS Release 11.0 or later, or the **write memory** command if you are running a Cisco IOS release earlier than 11.0:

```
Hostname# copy running-config startup-config
```

Taking this step will save the configuration settings that the AutoInstall process created in the access server. If you fail to do this, your configuration will be lost the next time you reload the access server.

Configuring the Access Server Manually Using the Setup Facility

If you do not plan to use AutoInstall, do not connect the access server's serial (WAN) cable to the channel service unit/data service unit (CSU/DSU). This will prevent the access server from attempting to run the AutoInstall process. The access server will attempt to run AutoInstall whenever you start it if the serial (WAN) connection is connected on both ends and the access server does not have a configuration stored in NVRAM. It can take several minutes for the access server to determine that AutoInstall is not set up to a remote TCP/IP host.

Once the access server has determined that AutoInstall is not configured, it will default to the setup facility. If the serial (WAN) cable is not connected, the access server will boot from Flash memory and go into the setup facility.

Note You can run the setup facility any time you are at the enable prompt (#) by entering the command **setup**.

Configuring the Global Parameters

When you first start the setup program you must configure the global parameters. The global parameters are used for controlling system-wide settings. Use the following procedure to enter the global parameters:

Step 1 Connect a console terminal by following the instructions in the section "Connecting the Console Terminal and Modem" in the chapter "Installing the Cisco 2500 Series Access Server" and then boot the access server to the EXEC prompt (Router>).

Step 2 When you have booted from Flash memory, the following information will appear after about 30 seconds. When you see this information displayed, you have successfully booted your access server:

```
System Bootstrap, Version 4.14(8), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
2500 processor with 16384 Kbytes of main memory

Loading igs-c-l.110-0.7 at 0x3000040, size = 3865444 bytes [OK]

F3: 3779532+85880+173868 at 0x3000060
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

```
            cisco Systems, Inc.
            170 West Tasman Drive
            San Jose, California 95134-1706


Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-C-L), Version 11.0(0.8), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Mon 19-Jun-95 23:22 by
Image text-base: 0x030200E4, data-base: 0x00001000

cisco 2500 (68030) processor (revision C) with 16380K/2048K bytes of
memory.
Processor board ID 2685538369
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software (copyright 1994 by TGV Inc).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Bridging software.
Authorized for Enterprise software set.  (0x0)
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
8 terminal lines.
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read ONLY)

Notice: NVRAM invalid, possibly due to write erase.

         --- System Configuration Dialog ---


At any point you may enter a question mark '?' for help.
Refer to the 'Getting Started' Guide for additional help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

Step 3 Enter **yes** or press **Return** when you are asked if you would like to enter the configuration dialog and if you would like to see the current interface summary. Press **Return** to accept the default (yes):

```
Would you like to enter the initial configuration dialog? [yes]:

First, would you like to see the current interface summary? [yes]:

Any interface listed with OK? value "NO" does not have a valid
configuration
```

```
Interface    IP-Address      OK?  Method     Status  Protocol
Ethernet0    unassigned      NO   not set    up      down
Serial0      unassigned      NO   not set    down    down
Serial1      unassigned      NO   not set    down    down
```

Step 4 Choose what protocols to support on your Ethernet or Token Ring interface. For IP-only installations, you can accept the default values for most of the questions. A typical configuration using IP, IPX, and AppleTalk follows:

```
Configuring global parameters:

  Enter host name [Router]: router
```

Step 5 Enter the enable secret password, the enable password, and the virtual terminal password:

```
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.

  Enter enable secret : shovel

The enable password is used when there is no enable secret
and when using older software and some boot images.

  Enter enable password : trowel
    Enter virtual terminal password: pail
```

Enter **yes** or **no** to accept or refuse SNMP management:

```
  Configure SNMP Network Management? [no]:
```

The Simple Network Management Protocol (SNMP) is the most widely supported open standard for network management. It provides a means to access and set configuration and run-time parameters of routers and communication servers. SNMP defines a set of functions that can be used to monitor and control network elements.

Step 6 Determine if you will be using DECnet on your access server. If you are configuring for DECnet, enter the appropriate values for your area number, node number, and area routing:

```
  Configure DECnet? [no]:
```

Step 7 In most cases you will use IP routing. If you are using IP routing, you must also select an interior routing protocol. You can specify only one of two interior routing protocols to operate on your system using setup: Interior Gateway Routing Protocol (IGRP) or Routing Information Protocol (RIP).

Enter **yes** (the default) or press **Return** to configure IP, and then select an interior routing protocol for IP:

```
Configure IP? [yes]:
  Configure IGRP routing? [yes]:
    Your IGRP autonomous system number [1]: 15
```

Step 8 In this example, routing will be enabled on AppleTalk and IPX; IP has already been selected:

```
Configure AppleTalk? [no]: yes
    Multizone networks? [no]: yes

Configure LAT? [yes]: no
Configure IPX? [no]: yes
```

Configuring the Asynchronous Interface

The access server is equipped with up to 16 asynchronous interfaces, which are referred to as lines in the setup dialog. The asynchronous lines must be configured to permit asynchronous devices to be connected to the access server. (See the sections "Asynchronous Protocols," and "Modems" in the appendix "Internetworking Primer.")

The asynchronous ports on the access server are configured to allow connection by TTY devices, Remote nodes, and Remote LANs.

A variety of devices can connect to the access server using the asynchronous lines. Terminals and remote nodes (such as PCs, Macintosh computers, workstations, and host systems) connect to the access server and make use of its services. The access server provides services allowing access to other asynchronous devices, such as printers, modems, or terminals.

The following steps configure the lines on the access server to permit use of the asynchronous lines by the access server or remote devices:

Step 1 Enter **yes** or press **Return** to configure asynchronous lines:

```
Configure Async lines? [yes]:
```

Step 2 Set the line speed and the flow control for the asynchronous lines. Hardware flow control must be configured to allow proper communications with modems.

```
Async line speed [9600]:57600
Configure for HW flow control? [yes]:
```

For additional information on configuring modem connections see the section "Modems" in the appendix "Internetworking Primer."

Step 3 Enter **yes** if you will be connecting modems to your access server to allow remote sessions, and to configure your modems to use the default chat script:

```
Configure for modems? [yes/no]: yes
   Configure for default chat script? [yes]:
```

Step 4 Configure your system to allow serial line internet protocol (SLIP) and Point-to-Point protocol (PPP) access, as follows:

```
Configure for Dial-in IP SLIP/PPP access? [no]: yes
  Configure for Dynamic IP addresses? [yes]: no
  Configure Default IP addresses? [no]: yes
  Configure for TCP Header Compression? [yes]:no
  Configure for routing updates on async links? [no]:
```

For additional information on configuring SLIP and PPP connections, see the section "Asynchronous Protocols" in the appendix "Internetworking Primer."

Step 5 Enter **yes** or press **Return** at the AppleTalk remote access prompt to configure for AppleTalk, and then enter the AppleTalk network address and zone name for your AppleTalk clients.

```
Configure for Appletalk Remote Access? [yes]:
  AppleTalk Network for ARA clients [1]: 99
  Zone name for ARA clients [ara-dialins]:
```

ARA protocol uses an internal nonextended unique network number, and a zone name for ARA protocol clients. For additional information on configuring ARA protocol, see the section "Asynchronous Protocols" in the appendix "Internetworking Primer."

Step 6 Enter **yes** if you will be using IPX on your asynchronous lines, In this example, the access server will not be using IPX on the asynchronous lines:

```
Configure XRemote font servers? [no]:
Configure for Async IPX? [yes]: no
```

Configuring the Ethernet or Token Ring Interfaces

Take the following steps to configure the Ethernet or Token Ring interface to allow communication over a LAN. To configure the interface parameters, you need to know your Ethernet or Token Ring interface network addresses.

Step 1 In the following example, the system is being configured for an Ethernet LAN using IP. Respond as follows (using your own addresses and mask) to the setup prompts:

```
Configuring interface parameters:

Configuring interface Ethernet0:
  Is this interface in use? [yes]:
 Configure IP on this interface? [yes]:
    IP address for this interface: 172.16.72.1
    Number of bits in subnet field [0]: 8

   Class B network is 172.16.0.0, 8 subnet bits; mask is 255.255.255.0
```

Step 2 Enter **yes** if you will be using AppleTalk on the interface, enter **yes** to configure for extended AppleTalk networks, and then enter the cable range number. See the appendix "Internetworking Primer" for additional information on AppleTalk routing. Enter the zone name, and any other additional zones that will be associated with your local zone:

```
Configure AppleTalk on this interface? [no]: yes
    Extended AppleTalk network? [no]: yes
    AppleTalk starting cable range [0]: 1
    AppleTalk ending cable range [1]: 2

    AppleTalk zone name [myzone]:
    AppleTalk additional zone name: otherzone
    AppleTalk additional zone name:
```

Step 3 Determine if you are going to enable IPX on this interface, enter the unique IPX network number. See the appendix "Internetworking Primer" for additional information on IPX routing:

```
Configure IPX on this interface? [no]: yes
    IPX network number [1]: B001
Configure XNS on this interface? [no]
```

Configuring the Synchronous Serial Interfaces

The synchronous serial interfaces are configured to allow connection to WANs through a CSU/DSU. Once the Ethernet or Token Ring port on your access server has been configured, take the following steps to configure the serial port:

Step 1 Enter **yes** to configure serial port 0:

```
Configuring interface Serial0:
  Is this interface in use? [no]: yes
```

Step 2 Determine what protocols you will allow on the synchronous serial interface and enter the appropriate responses:

```
Configure IP unnumbered on this interface? [no]: no
    IP address for this interface: 172.16.73.1
    Number of bits in subnet field [8]:
Class B network is 172.16.0.0, 8 subnet bits; mask is 255.255.255.0

Configure AppleTalk on this interface? [no]: yes
    Extended AppleTalk network? [yes]:

    AppleTalk starting cable range [2]: 3
    AppleTalk ending cable range [3]: 3

    AppleTalk zone name [myzone]: ZZ Serial
    AppleTalk additional zone name:

Configure IPX on this interface? [no]: yes
    IPX network number [2]: B000
```

Step 3 Configure the second synchronous serial interface as follows:

```
Configuring interface Serial1:
  Is this interface in use? [no]:
```

```
Configure IP unnumbered on this interface? [no]: yes
    IP address for this interface: 172.16.74.2
    Number of bits in subnet field [8]:
Class B network is 172.16.0.0, 8 subnet bits; mask is 255.255.255.0

 Configure AppleTalk on this interface? [no]: yes
    Extended AppleTalk network? [yes]:
    AppleTalk starting cable range [2]: 4
    AppleTalk ending cable range [3]: 4

    AppleTalk zone name [myzone]: ZZ Serial
    AppleTalk additional zone name:

 Configure IPX on this interface? [no]: yes
    IPX network number [2]: B002
```

Entering the Asynchronous Interface Addresses

After the asynchronous lines have been configured and the routing protocols have been selected, enter the IP addresses for each asynchronous interface.

For information on asynchronous protocols, see the section “Asynchronous Protocols” in the appendix “Internetworking Primer,” and for information on IP addressing, see the section “Desktop Protocols” in the appendix “Internetworking Primer.”

Step 1 Enter the IP address for each of the asynchronous interfaces on the access server:

```
Configuring interface Async1:
   Default client IP address for this interface [none]: 172.16.72.11

Configuring interface Async2:
    Default client IP address for this interface [172.16.72.12]:

Configuring interface Async3:
    Default client IP address for this interface [172.16.72.13]:

Configuring interface Async4:
    Default client IP address for this interface [172.16.72.14]:

Configuring interface Async5:
    Default client IP address for this interface [172.16.72.15]:
```

```
Configuring interface Async6:
    Default client IP address for this interface [172.16.72.16]:

Configuring interface Async7:
    Default client IP address for this interface [172.16.72.17]:

Configuring interface Async8:
    Default client IP address for this interface [172.16.72.18]:
```

Step 2 The configuration you have entered is now displayed and you are asked if you want to use the displayed configuration. If you answer **no**, you can begin the configuration again. If you answer **yes**, the configuration will be entered and saved in the startup configuration:

```
Use this configuration? [yes/no]:yes

Press RETURN to get started!

[OK]

Use the enabled mode 'configure' command to modify this
configuration.
```

The access server is now configured properly and is ready to use. Enter the command **setup** if you want to modify the parameters after the initial configuration. To perform more complex configurations, enter the command **configure**. For information on configuration, see the publication *Access and Communications Servers Configuration Guide*.

Checking Your Settings

You can check the value of the settings you have entered by entering at the # prompt the command **show running-config** if you are running Cisco IOS Release 11.0 or later, or the command **write terminal** if you are running a Cisco IOS Release earlier than 11.0:

```
router# show running-config
.
.
.
configuration register is 0x2102
```

To store the configuration or changes to your startup configuration, enter at the hostname# prompt the command **copy running-config startup-config** if you are running Cisco IOS Release 11.0 or later, or the command **write memory** if you are running a Cisco IOS release earlier than 11.0:

```
Hostname# copy running-config startup-config
```

Entering this command will save the configuration settings that the setup process created in the access server. If you fail to do this, your configuration will be lost the next time you reload the access server.

APPENDIX A

Internetworking Primer

This appendix gives an introduction to the technologies used in internetworking. It also includes basic information about designing and implementing an internetwork with a Cisco 2500 series access server.

The appendix includes primers on the following topics:

- Cisco Internetwork Operating System
- LANs and WANs
- Desktop Protocols
- Modems
- Asynchronous Protocols

These primers give a brief introduction to the technologies involved in building an internetwork solution. For more information, see the following publications:

- *Access and Communication Servers Configuration Guide*
- *Access and Communication Servers Command Reference*
- *Router Products Getting Started Guide*
- *Router Products Configuration Guide*
- *Troubleshooting Internetworking Systems*
- *Internetworking Technology Overview*
- *Internet Design Guide*
- *Internetwork Case Studies*

Note To order UniverCD, Cisco's technical documentation in CD-ROM format, or paper documentation, refer to "Ordering Cisco Documents," DOC-OCD, which is in your warranty pack.

Cisco Internetwork Operating System

This primer will help you become familiar with using Cisco Internetwork Operating System (Cisco IOS) software, including the following features:

- Internal memory components
- Cisco IOS operating environments
- Command modes
- Configuration files

Refer to the chapters "Understanding the User Interface," "Loading System Images and Configuration Files," "Configuring Terminal Lines and Modem Support," and "Managing the System" in the publication *Access and Communication Servers Configuration Guide*.

Internal Memory Components

The Cisco 2500 series access server has several kinds of memory—read-only memory (ROM), Flash memory, nonvolatile random access memory (NVRAM), random access memory (RAM), and shared-packet memory. System software images, configuration files, and transient data structures such as routing tables and packets are stored in memory. Table A-1 lists the different kinds of memory and indicates what they are used for.

Table A-1 Internal Memory Components

Memory	Purpose
ROM	Stores the ROM Monitor, and boot ROM
Flash memory	Stores the system image (Cisco IOS)
NVRAM	Stores the configuration file (startup-config)

Memory	Purpose
RAM	Stores the operating configuration (for example, running-config), routing tables, caches, queues, packets, and so forth
Shared packet memory	Stores incoming and outgoing packets

The **show version** command displays the capacity of each kind of memory.

Proper operation of the access server requires the following memory configuration:

- The correct system image (Cisco IOS) is loaded and running in Flash memory. See the following section "Cisco IOS Operating Environments."
- The proper configuration file is loaded into RAM. See the section "Configuration Files" later in this appendix.

Cisco IOS Operating Environments

The access server has three distinct operating environments (see Table A-2).

Table A-2 Cisco IOS Operating Environments

Operating Environment	Prompt	Configuration Register	Usage
ROM monitor	>	0x0	Failure or password recovery
Boot ROM	Router(boot)>	0x1	Flash image upgrade
Cisco IOS	Router>	0x2102	Normal operation

The startup process of the access server normally loads and executes each of the operating environments in turn.

The configuration register can be used by system administrators to control some very low level operations of the access server. When the configuration register is set to specific values (shown in Table A-2), the access server can be instructed to stop the boot process in any of the three operating environments. You modify the configuration register value by using the configuration command **config-reg** *[value]*.

ROM Monitor

ROM monitor performs the bootstrap process and provides low-level diagnostics. You cannot use ROM monitor to operate any of the interfaces. You can only access ROM monitor via the console port. Setting the configuration register value to 0x0 and reloading causes the access server to operate in the ROM monitor environment. The ROM monitor is used to recover from system failures, and to recover a lost password.

Boot ROM

Boot ROM is used primarily to modify the Cisco IOS image that is loaded into Flash memory. Flash memory is read-only when you are running the Cisco IOS software from Flash memory; boot ROM allows write operations to Flash memory. If you are running in boot ROM, only a limited subset of the Cisco IOS feature set is available. For example, boot ROM does not support IP routing or subinterfaces. You can set the configuration register value to 0x1 and reload to cause the access server to operate in the boot ROM environment.

Timesaver Enter the configuration command **ip default-gateway** [*ipaddress*] to tell Cisco IOS software where to send IP packets when you are running from boot ROM if the destination address is not directly connected. This command can be left in the configuration file while you are running from Flash memory because it will be ignored when IP routing is enabled.

You can modify the Cisco IOS image if you are running in boot ROM by entering the command **copy tftp flash**. You can also modify Flash memory while running from Flash memory by entering the command **partition flash** or using Flash Load Helper. See the publication *Access and Communication Servers Configuration Guide* for more information.

Cisco IOS

Normal operation of your access server requires the Cisco IOS image to be stored and executing in Flash memory. A recommended setting for the configuration register value is 0x2102, which instructs the access server when it boots to do the following:

- Operate the image in Flash memory
- Ignore the Break key on the console port
- Attempt to load the Flash image only five times before reverting to boot ROM

Enter the command **show version** to display the Cisco IOS image and version that the access server is running:

```
Router#show version
Cisco Internetwork Operating System Software
Cisco IOS (tm) 3000 Software (IGS-C-L), Version 10.2(6), RELEASE SOFTWARE
(fc2)
...
```

Command Modes

The Cisco IOS user interface provides several different command modes. Each command mode provides a group of related commands. Table A-3 summarizes the key command modes and their purpose.

Table A-3 Key Command Modes and Their Purpose

Command Mode	Prompt	Purpose	How
User EXEC	Router>	User access	First level accessed
Privileged EXEC	Router#	System administration	Enter the command **enable**
Configuration mode	Router(config)#	Modify configuration	Enter the command **config**
Setup	Prompted dialog	Create the initial configuration	Enter the command **setup**

EXEC Modes

The command interpreter of Cisco IOS software is called the EXEC. The EXEC interprets the commands you type and carries out the corresponding operations. You must log in to the access server before you can enter an EXEC command. For security purposes, the EXEC has two basic levels of access to commands, user EXEC mode and privileged EXEC mode.

In both EXEC modes, you can find what commands are currently available by entering a question mark (?), as follows:

```
Router>?
EXEC commands:
  connect          Open a terminal connection
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
...
```

To display more detail about a command, enter the command followed by a ?, as follows:

```
Router>connect ?
  WORD  IP address or hostname of a remote system
```

User EXEC Mode

When you connect to the access server (through a console, a Telnet connection, or a dial-in connection) you are started in user EXEC mode. In general, the user EXEC commands allow you to connect to other network devices, change terminal settings on a temporary basis, perform basic tests, and list system information. The user EXEC commands are a subset of the privileged EXEC commands.

Privileged EXEC Mode

From user EXEC mode, enter the EXEC command **enable** to enter privileged EXEC mode.

The privileged command set includes all the commands that are available in user EXEC mode plus the **configure** command, debugging commands, and the **setup** command. Because many of the privileged commands allow you to set operating system parameters, privileged EXEC mode should be password-protected to prevent unauthorized use (see the

section "Using the Enable Secret and the Enable Password," in the chapter "Configuring the Cisco 2500 Series Access Server"). Enter **?** to display the privileged commands. Privileged commands include the following:

- **configure**—Changes the access server's software configuration.
- **debug**—Displays process and hardware event messages. Use caution with the **debug** command because the additional load of generating debug message can overload the CPU.
- **setup**—Enter configuration information at the prompts.

Enter the command **disable** to exit from the privileged EXEC mode and return to user EXEC mode.

Configuration Mode

You use configuration mode to configure the access server. You can use configuration mode for initial setup of the system (using the subcommand **setup**), as well as to change settings after initial setup, either permanently or temporarily.

Configuration mode has a set of submodes that you use for modifying interface settings, routing protocol settings (such as Interior Gateway Routing Protocol (IGRP), or Open Shortest Path First (OSPF)), line settings, and so forth. Use caution with configuration mode because all changes you enter take effect immediately.

Enter the command **configure terminal** to enter configuration mode and exit by pressing **Ctrl–Z**. The following is a sample configuration session:

```
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterA
RouterA(config)#interface e 0
RouterA(config-if)#description Floor 2 LAN
RouterA(config-if)#^Z
RouterA#
```

Setup Mode

You use the setup facility of Cisco IOS software to streamline the creation of configuration files. If Cisco IOS software determines that there is no configuration file stored in NVRAM, it will automatically enter setup mode when the access server boots. (See the section "Configuring the Access Server Manually Using the Setup Facility" in the chapter "Configuring the Cisco 2500 Series Access Server" for more information about the **setup** command.)

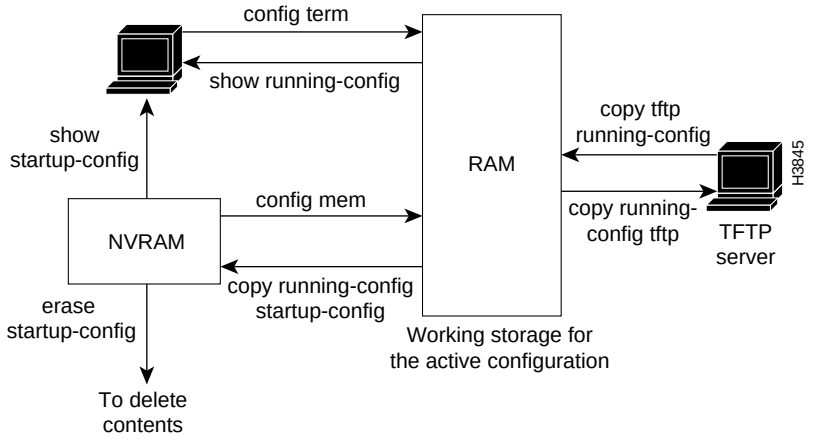
Configuration Files

You need to create and store a configuration file in order to use the access server. The configuration file contains commands that enable protocol routing, assign addressing, perform security, and so forth. Use the following privileged mode commands to work with configuration files on the access server:

- **configure terminal**—Modify the running configuration manually from the terminal.
- **show running-config** (Cisco IOS Release 11.0 or later) or **write terminal** (earlier than Cisco IOS Release 11.0)—Display the running configuration.
- **configure memory**—Load the configuration from NVRAM to RAM. This takes place automatically when the system starts up.
- **copy running-config startup-config** (Cisco IOS Release 11.0 or later) or **write memory** (earlier than Cisco IOS Release 11.0)—Copy the running configuration in RAM into the startup configuration in NVRAM.
- **copy tftp running-config** (Cisco IOS Release 11.0 or later) or **configure network** (earlier than Cisco IOS Release 11.0)—Load a configuration file stored on a Trivial File Transfer Protocol (TFTP) server into the running configuration.
- **copy running-config tftp** (Cisco IOS Release 11.0 or later) or **write network** (earlier than Cisco IOS Release 11.0)—Store the running configuration on a TFTP server.
- **show startup-config** (Cisco IOS Release 11.0 or later) or **show configuration** (earlier than Cisco IOS Release 11.0)—Display the saved configuration in NVRAM.
- **erase startup-config** (Cisco IOS Release 11.0 or later) or **write erase** (earlier than Cisco IOS Release 11.0)—Erase the contents of NVRAM. If you enter the **reload** command after the **erase startup-config** (or **write erase**) command, the access server will not have a running configuration.

The interaction of the configuration commands is illustrated in Figure A-1.

Figure A-1 Configuration Command Interaction with Cisco IOS Release 11.0



LANs and WANs

This section briefly describes the common local-area network (LAN) and wide-area network (WAN) technologies you may encounter when you are building an internetwork. An important function of an access server is to interconnect LANs and WANs.

To understand LANs and WANs, you should be familiar with the Open System Interconnection (OSI) reference model of networks. The OSI reference model is a seven-layer model designed by the International Organization for Standardization (ISO) and the International Telecommunications Union Standardization Sector (ITU-T) to aid in the development and understanding of computer networking and communications. The OSI reference model divides the issue of moving information between computers into seven layers.

Each layer of the OSI reference model specifies particular network functions such as addressing, flow control, error control, encapsulation, reliable message transfer, and data representation. The upper layer (the application layer) is closest to the user; the lowest layer (the physical layer) is the closest to the cables and wires.

Each layer of the OSI reference model relies on the layers below, and offers its services to the layers above.Table A-4 summarizes the layers and their functionality.

Table A-4 OSI Reference Model of Networks

Layer	Title	Purpose	Example
7	Application	Services to users	File transfer, e-mail, virtual terminals
6	Presentation	Data representations	ASCII text, EBCDIC[1], ASN.1
5	Session	Control of sessions	Printing, file sharing
4	Transport	Reliable delivery of packets over networks	TCP[2], SPX[3], ATP[4], and ADSP[5]
3	Network	Logical addressing, routing	IP, IPX[6], AppleTalk DDP[7]
2	Data link	Physical addressing, topology (bus or ring), line access method	Ethernet, Token Ring, HDLC[8], PPP[9]
1	Physical	Electrical, mechanical	10BaseT, 10Base2

1. EBCDIC = Extended Binary Coded Decimal Interchange Code.
2. TCP = Transmission Control Protocol.
3. SPX = Sequenced Packet Exchange.
4. ATP = AppleTalk Transaction Protocol.
5. ADSP = AppleTalk Data Stream Protocol.
6. IPX = Internetwork Packet Exchange.
7. DDP = Datagram Delivery Protocol.
8. HDLC = High-Level Data Link Control.
9. PPP = Point-to-Point Protocol.

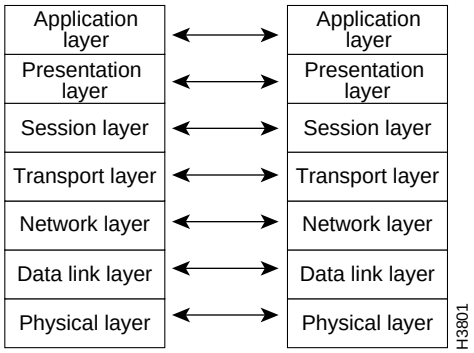
LANs and WANs are generally defined by the lower two layers of the OSI reference model. Higher layer protocols (such as TCP/IP, IPX, or AppleTalk) can use the foundation laid at the lower layers to transport data between network devices.

For example, the IEEE standard 802.3 (Ethernet) defines the physical layer (connectors, voltages, and binary logic to enable communication) as well as the data link layer (framing data structures, addressing packets for local delivery, and error checking).

Once the physical and data link layers are installed in a network and working correctly, the network layer and its associated devices can use these services to route packets efficiently across the room or around the world.

Building a network involves understanding the OSI reference model in each portion of the network. Sketching the model out on paper is a great help in designing, administering, and troubleshooting networks. (See Figure A-2.)

Figure A-2 The OSI Reference Model



LAN Technologies

LANs operate at Layer 1 (the physical layer) and Layer 2 (the data link layer) and are usually used to connect computing devices within a single building. For example, a LAN in a small office may include three PCs, a print server, and a file server.

The three most common physical LAN implementations are Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI). These implementations have been standardized by Institute of Electrical and Electronic Engineers (IEEE) and the American National Standards Institute (ANSI).

Ethernet LANs

The IEEE has established Ethernet as standard 802.3. Ethernet uses a 10-Mbps bus. Ethernet LANs use carrier sense multiple access collision detect (CSMA/CD) for bus access control. Several physical layer implementations have been established for Ethernet; the more common implementations are as follows:

- 10Base5—Ethernet on thick coaxial cable. This implementation was based on the original Ethernet and is not in common use today. Maximum segment length is 1,640 feet (500 m).
- 10Base2—Ethernet on thin coaxial cable. 10Base2 cabling is similar in appearance to TV cable, but uses a different specification. Maximum segment length is 656 feet (200 m).
- 10BaseT—Ethernet on unshielded twisted-pair (UTP) wiring. 10BaseT is similar to the wiring used for phones, but must meet certain electrical standards in order to be used. Maximum segment length is 328 feet (100 m).

Configuring Ethernet

Special configuration commands are not required for the Ethernet interface on the Cisco 2500 series access server. The Ethernet configuration commands are as follows:

- **show interface**—an EXEC command that displays information about the interfaces attached to the access server.
- **[no] shutdown**—a **config-interface** subcommand, that enables or disables operation of the configured interface.

Token Ring LANs

The IEEE has established Token Ring as standard 802.5. Different physical implementations of Token Ring are available, including variations on shielded twisted-pair (STP) and UTP cabling. Token Ring is very common in IBM environments.

Token Ring can operate at two different ring speeds: 4 Mbps and 16 Mbps. All devices on the ring must agree on the operating speed.

Configuring Token Ring

The only option you must configure Token Ring interfaces is the ring speed. The following example shows the commands you typically enter to configure the ring speed on a Token Ring network:

```
Router(config)# interface tokenring 0
Router(config-if)# ring-speed 16
```

Other useful commands are:

- **show interface**—an EXEC command that displays information about interfaces attached to the access server.
- **[no] shutdown**—a **config-interface** subcommand, that enables or disables operation of the configured interface.

Timesaver You may also need to enter the command **multiring** if the Token Ring interface on the access server is sending routed packets (such as IP, IPX, or AppleTalk) to a source-route bridged environment. The command **multiring** tells the access server or router to try to find devices on the other side of source-route bridges.

LAN Addressing

The data link layer defines an addressing scheme that is used by all LAN devices. A device's address is generally burned into the chips on the network interface components that connect the device to the LAN. These addresses are 48-bits in length, which is represented by a hexadecimal string (for example, 0000.0C0A.3E2E).

The IEEE provides each manufacturer of network interface cards with a block of addresses, and the manufacturers program the cards they make with these unique addresses. These addresses are called Media Access Control (MAC) addresses, since MAC is a sublayer within Layer 2 of the OSI reference model.

Cisco products use addresses from the pool 0000.0Cxx.xxxx for all devices and all interfaces. Enter the EXEC command **show interface** to see the Layer 2 address:

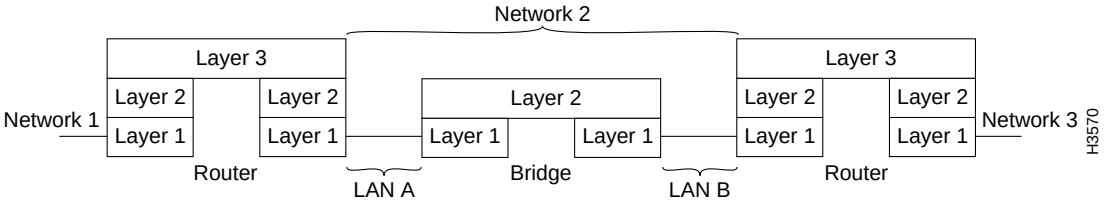
```
Router# show interface
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0000.0c14.2622 (bia 0000.0c14.2622)
```

In addition to data link layer addressing, network protocols (Layer 3) were developed to allow more precise delivery of packets (or routing), within a larger internetwork. This strategy is similar to the post office's method of delivering mail. Everyone has a name (like a MAC address), but that is not enough information to route letters efficiently. Zip codes (like Layer 3 addresses) help mail reach its exact destination more efficiently by routing them through the national mail infrastructure.

Bridged LANs

You can use data link layer bridges to extend the physical distance limitations of LANs. (See Figure A-3.) It is important to note that the network layer logical addressing is not affected by bridges, and network layer devices (such as access servers and routers) treat a bridged Ethernet or bridged Token Ring as one data link for addressing purposes. The two common kinds of bridges are transparent and source-route bridges.

Figure A-3 Two LANs Connected with a Bridge to Form Network 2



Translational bridging between two dissimilar LANs such as a Token Ring LAN and an Ethernet LAN can cause problems for some Layer 3 protocols like AppleTalk and IPX. Translational bridging should only be implemented after careful design consideration.

WAN Technologies

WANs connect networks together across longer distances, such as between cities, or across continents. Figure A-4 illustrates a typical WAN architecture.

Figure A-4 A Typical WAN Architecture

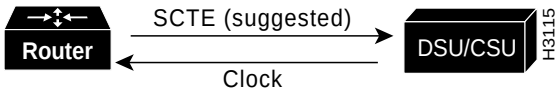
WAN Physical Layer (Layer 1)

Most WANs require an interconnection that is provided by a communications service provider, such as a phone company. This physical layer uses many of the technologies that have evolved over the last few decades for carrying voice communications. The service provider circuit typically terminates at a channel service unit (CSU) at the customer site.

Master Clock Timing

Two communicating devices on a synchronous serial cable, such as a CSU and an access server, must agree on which device will provide the clocking for data transmission timing. That device (typically an external channel service unit/data service unit [CSU/DSU]) is called data circuit-terminating equipment (DCE). The other device will be data terminal equipment (DTE), and is usually an access server or router. The physical layer connectors (such as EIA/TIA-232 or V.35) together with the mode (DTE or DCE) will determine the required pinout on the cable connecting the two devices. (See Figure A-5.)

Figure A-5 Master Clock Timing



Note The cable used on the access server port will configure the port as DTE or DCE. If it is configured as DCE, enter the command **clockrate** *value* to enable the port for use as a DCE port.

Some WAN technologies, such as Frame Relay, Switched Multimegabit Data Service (SMDS), or X.25, reuse the DTE and DCE terminology at Layer 2. The DTE/DCE mode at Layer 1 is independent of the DTE/DCE mode at Layer 2. For example, It is possible for a single device to be a V.35 DTE and a Frame Relay DCE concurrently.

If the access server is configured as a DTE (default) and is correctly receiving clocking and Carrier Detect (CD) signals from the CSU, the command **show interface** will display the following information:

```
Router# sh interface
Serial0 is up, line protocol is down
```

Note In this example, the Serial 0 interface is up, but the line protocol is reported to be down. For the line protocol to be up, the WAN data link (Layer 2) must also be operational.

WAN Data Link Layer

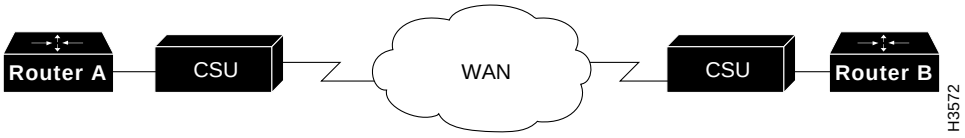
The WAN data link layer (Layer 2), defines how data is formatted, or framed, for transmission to remote sites. This formatting is referred to as encapsulation. Common WAN encapsulations include High-Level Data Link Control (HDLC), Point-to-Point protocol (PPP), Frame Relay, and SMDS.

WAN Layer 2 technologies can be grouped into two categories: point-to-point HDLC and PPP) and multipoint (Frame Relay, SMDS, X.25, and Asynchronous Transfer Mode (ATM)). Each category has its own specific design considerations. Multipoint technologies can also be used in point-to-point topologies.

Point-to-Point WANs

Point-to-point WANs only allow two endnodes on the WAN connection (as shown in Figure A-6). The two common point-to-point WAN encapsulations are HDLC and PPP. Because there are only two devices, there is no need for addressing at the data link layer. Point-to-point encapsulations are generally used on leased WAN lines.

Figure A-6 Point-To-Point WAN



High-Level Data Link Control

If both ends of a leased-line connection are routers or access servers running Cisco IOS software, HDLC encapsulation is typically used. As HDLC encapsulation methods may vary, use PPP with devices that are not running Cisco IOS software.

HDLC is a bit-oriented, data link layer protocol derived from the Synchronous Data Link Control (SDLC) encapsulation protocol. HDLC provides an encapsulation method for synchronous serial links with a 32-bit checksum.

The serial interface on the access server does not require special configuration because HDLC encapsulation is configured as the default.

Point-to-Point Protocol

PPP encapsulation provides Cisco IOS software to devices that are not running Cisco IOS software, connectivity over leased WAN lines. PPP uses a more complex model than HDLC to ensure interoperability between networking vendors. This interoperability involves several additional protocols, including the following:

- Link control protocol for negotiating basic line interoperability
- A family of network control protocols for negotiating individual Layer 3 protocols and their options (such as IPCP for IP and options such as compression)

When the PPP link is negotiated, a link control protocol is negotiated to establish the link and then additional network control protocols are negotiated. If IP, AppleTalk, or IPX, are configured on the serial line, IP control protocol (IPCP), AppleTalk control protocol (ATCP), or IPX control protocol (IPXCP), respectively, is negotiated to conform to the protocols requirements.

Enter the command **show interface** to check the status of the link control protocol and the network control protocol, and test the interoperability of the network layers. There are also excellent **debug ppp** commands for troubleshooting. (See the publication *Access and Communication Servers Command Reference*.)

To configure the serial line to use PPP, enter the interface subcommand **encapsulation ppp** as follows:

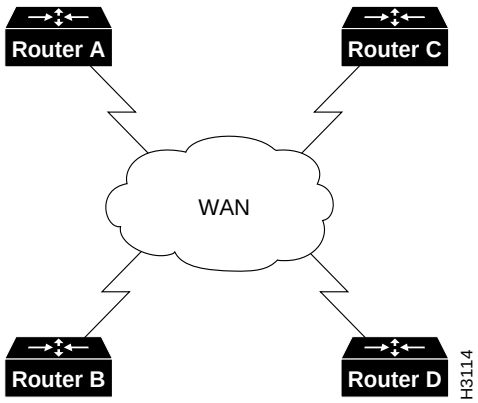
```
Router(config)# interface s0
Router(config-if)# encapsulation ppp
```

Multipoint WAN Technologies

Advances in technology over the last decade have resulted in a number of additional WAN solutions being available to network designers. These sections include multipoint WAN technologies such as Frame Relay, SMDS, X.25, and ATM. (See Figure A-7.)

Selection of an appropriate WAN solutions should involve a discussion of the costs and benefits of each with your network designer and service providers.

Figure A-7 Multipoint WAN



Frame Relay

Frame Relay is a packet-switching data communications technology that can connect multiple network devices on a multipoint WAN. The design of Frame Relay WANs can have impact on aspects of higher layer protocols such as IP, IPX, and AppleTalk (for example, the split-horizon aspect of routing protocols). Frame Relay is called a nonbroadcast multiaccess technology, because there is no broadcast channel. Broadcasts are transmitted by sending packets to all network destinations.

Two common topologies that can be used in a Frame Relay solution:

- Fully meshed topology

  Every Frame Relay network device has a permanent virtual circuit (PVC) to every other device on the multipoint WAN. Any update sent by one device will be seen by every other. If this design is used, the entire Frame Relay WAN can be treated as one data link.

- Partially meshed topology

  This is also often called a “star” or “hub-and-spoke” topology. In a partially meshed topology, not every device on the Frame Relay cloud has a PVC to every other device. In this topology, subinterfaces should be investigated and probably implemented to solve design issues.

Frame Relay WANs should be carefully designed with the above considerations in mind. (see the publication *Internetwork Design Guide*).

Dial-on-Demand Routing

Dial-on-demand routing (DDR) enables you to make a standard telephone connection or an Integrated Services Digital Network (ISDN) connection only when required by the volume of network traffic. DDR may be less expensive than a leased-line or multipoint solutions.

See the publication *Access and Communication Servers Configuration Guide* for assistance in selecting, designing, and configuring dial-on-demand solutions.

Desktop Protocols

Desktop protocols are the network layer protocols that are commonly used by desktop workstations and are supported by the Cisco 2500 series access server. This section briefly describes the three most common desktop protocols—IP, IPX, and AppleTalk.

Network designers and administrators should be familiar with which networking functions are performed by the data link layer (Layer 2) and which are performed by the network layer (Layer 3) of the OSI reference model. For more information about the OSI reference model, see the section "LANs and WANs" earlier in this appendix.

IP, IPX, and AppleTalk are all defined as routed (or routable) protocols. The unique numbering of each network (data link) and the addressing of each data packet based on this numbering allow efficient packet routing through the internetwork. This is similar to the use of zip codes to allow efficient routing of mail through the national mail infrastructure.

This section includes the following information:

- The common design goals of each desktop protocol
- How each protocol meets these goals
- Example configurations of IP, IPX, and AppleTalk

Routed Protocol Design Goals

Each of these three desktop protocols was designed with a common set of goals—unique network numbering, node addressing, and data link address resolution, routing protocols, and directory services. Understanding these goals, and how each desktop protocol solves each goal, aids in the understanding, building, and administration of internetworks.

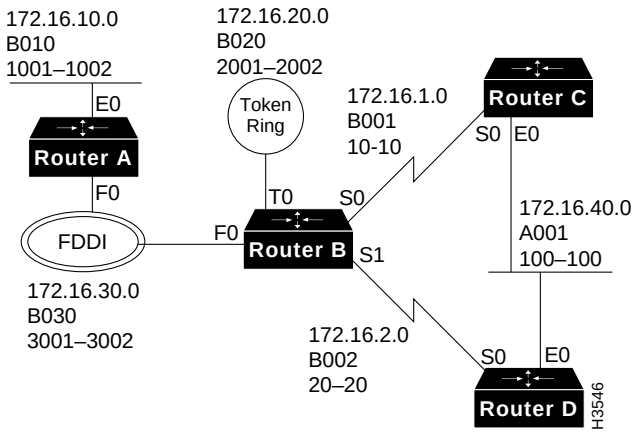
Unique Network Numbering

Every data link in your internetwork is given a unique network number. Every LAN (Ethernet or Token Ring), and WAN is assigned its own unique network number for identification. A bridged or switched LAN is only one network from the perspective of a network protocol. Routers and access servers use these network numbers to route packets within an internetwork. IP, IPX, and AppleTalk all use a similar model for assigning each distinct network a unique network number. Network administrators must develop a numbering plan for each protocol and control assignment of the unique network numbering. Duplicate network numbers in a routed network will cause loss of connectivity.

More than one protocol can be implemented on a network. The numbering plan for each network protocol is independent of the numbering plan used by other network protocols.

Figure A-8 illustrates a numbering plan for IP, IPX, and AppleTalk networks.

Figure A-8 Network Numbering Plan for IP, IPX, and AppleTalk



Node Addressing and Data Link Address Resolution

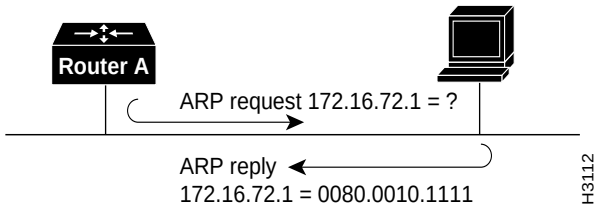
Each network protocol needs to able to uniquely address each node on a network. This network layer node address may be the same as, or independent of, the already unique data link layer address.

Once a packet has been routed to the correct network (data link), based on the network number, it must be delivered to the correct node. Delivery of the packet on a network is done using the Layer 2 (data link layer) address. A companion protocol performs resolution of Layer 3 node address to the Layer 2 data link address. This companion protocol is called the Address Resolution Protocol (ARP) for IP and AppleTalk Address Resolution Protocol (AARP) for AppleTalk. IP and AppleTalk both use ARPs but IPX does not, because the IPX 48-bit node address is always the same as the 48-bit data link address. The ARP must be working correctly in order to maintain connectivity between the devices in an internetwork.

The ARP (or AARP) address mapping process is illustrated in Figure A-9 and works as follows:

1. A node needs to deliver a packet to a network layer node address. It checks its ARP table to determine the data link address associated with the node address. If a mapping exists, it can deliver the packet. If a mapping does not exist, an ARP is performed.
2. To perform an ARP, the requesting node broadcasts an ARP request to all devices on the connected network to ask who has the specific node address.
3. The device with that node address sends a unicast (a message sent to a single network destination) ARP reply to the requesting node.
4. The requesting node adds the new mapping to its ARP table and delivers the packet.

Figure A-9 Address Resolution Protocol Mapping Process



Routing Protocols

Each network protocol has associated routing protocols that access servers and routers use to share information about network topologies. Over time, a number of routing protocol choices have evolved for each network protocol. Network designers should select the routing protocol for each network protocol.

The function of the routing protocol is to build a complete routing table in each access server or router. The routing table is a pointer to every network in an internetwork. For example, the IP routing table for Router B in Figure A-8 might look as follows:

```
network       cost       next hop      interface
172.16.10.0   01         RouterA       f0
172.16.20.0   00         connected     t0
172.16.30.0   00         connected     f0
172.16.1.0    00         connected     s0
172.16.2.0    00         connected     s1
172.16.40.0   01         RouterC       s0
172.16.40.0   01         RouterD       s1
```

In order to achieve two-way connectivity between two end nodes and therefore the ability to exchange packets on an internetwork, every access server or router in the path between the nodes must have a routing table entry that describes how to forward a packet addressed to both nodes. Connectivity also depends on the correct operation of ARP to deliver the packet within the networks at either end of the packet's path.

Directory Services

Nodes on an internetwork use directory services to locate specific services such as file servers, printers, and e-mail servers. Each protocol (IP, IPX, and AppleTalk) has a unique way of doing this. For IPX and AppleTalk, support of directory services is a critical part of the design considerations.

Internet Protocol

IP is used by the Internet (the world's largest internetwork, which connects thousands of networks worldwide) and within many companies. Its addressing scheme scales well for global addressing although, like the telephone industry, address space is running out.

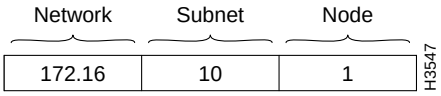
IP uses centrally administered major network numbers to allow internetworks to connect to the Internet. If you require Internet connectivity, you will need to get network address space from an organization called the InterNIC (the InterNIC controls address allocation for the Internet). If you do not plan to have Internet connectivity, or if you have limited assigned address space, see RFC 1597 for numbering suggestions.

Design and administration of an IP network requires an understanding of IP subnetting. Review the document *Beginning IP for New Users* which is available on CIO to ensure basic familiarity with the concepts of IP subnetting.

IP Network Numbering

The IP address space is 32 bits long and is used to represent both the network and the node. An IP address is written as four decimal numbers separated by dots (called dotted decimal notation); for example, 172.16.10.1. Each of the four numbers is called an octet because it represents 8 bits, and each octet has a maximum value of 255. For routing purposes, the IP address is broken into three parts: major network, subnet, and node. (See Figure A-10.)

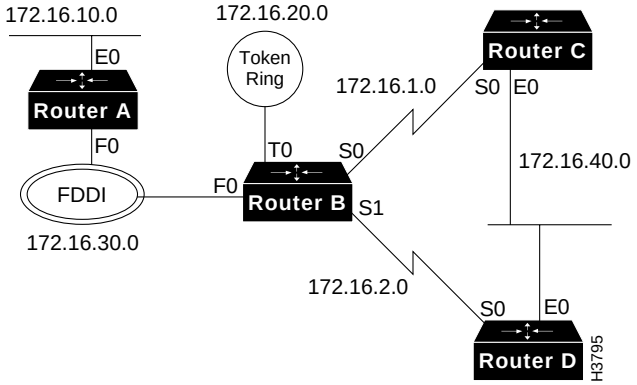
Figure A-10 IP Address Broken into Network, Subnet, and Node Fields



Major networks are allocated by the InterNIC to identify different internetworks that are connecting to the Internet. Subnets are used to number each data link (network) within an internetwork, and the bits to the right of the subnet field are used for the node address.

In Figure A-11, the major network is the class B network, 172.16.0.0. The subnet mask is 255.255.255.0. Networks are uniquely numbered at the third octet. In Figure A-11, subnets 1, 2, 10, 20, 30, and 40 have been assigned to the distinct networks.

Figure A-11 IP Subnetting Plan



IP Node Numbering

IP uses the bits to the right of the subnet mask to uniquely number each node on the network. These addresses are configured manually by the system administrator. Access servers and routers are also nodes, and require unique node addresses. In Figure A-11, the fourth octet is used to number the nodes on a subnet, which permits up to 254 nodes on each subnet (0 and 255 are reserved numbers).

IP ARP requires no special configuration, and will automatically perform Layer 2 address resolution for IP. Enter the command **show arp** to check the ARP table on the access server.

IP Routing Protocols

There are several routing protocol options for IP. Network designers should select which routing protocol to use, taking into consideration such factors as interoperability, convergence, performance, support of variable length subnet masks (VLSMs), and protocol overhead.

The IP routing protocol options are as follows:

- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced IGRP
- OSPF
- Integrated Intermediate System-to-Intermediate System (integrated IS-IS)
- Static routing (a fixed, configured routing table entry)

Enter the command **show ip route** to examine the IP routing table.

IP Directory Services

The directory service used with IP is called Domain Name System (DNS). DNS resolves names into IP addresses. Some useful configuration commands used with DNS are as follows:

- **ip name-server**
- **ip domain-name**
- **ip domain-lookup**

IP Configuration Example

The IP configuration of Router C in Figure A-11 is as follows:

```
interface ethernet 0
ip address 172.16.40.1 255.255.255.0
!
interface serial 0
ip address 172.16.1.1 255.255.255.0
!
router igrp 1
network 172.16.0.0
!
ip name-server 172.16.10.100
```

Because Router D and Router C share a data link, they must agree on the IP network and the subnet used on that data link, but they must have unique node numbers. The serial link used by Router D is distinct from the serial link used by Router C, so it uses a unique subnet number.

The IP configuration of Router D in Figure A-11 is as follows:

```
interface ethernet 0
ip address 172.16.40.2 255.255.255.0
!
interface serial 0
ip address 172.16.2.1 255.255.255.0
!
router igrp 1
network 172.16.0.0
!
ip name-server 172.16.10.100
```

Note IP hosts are usually configured with the IP address of the access server (or other IP router) set as a default gateway. For additional information, see the publication *Internetwork Design Guide*.

IPX Protocol

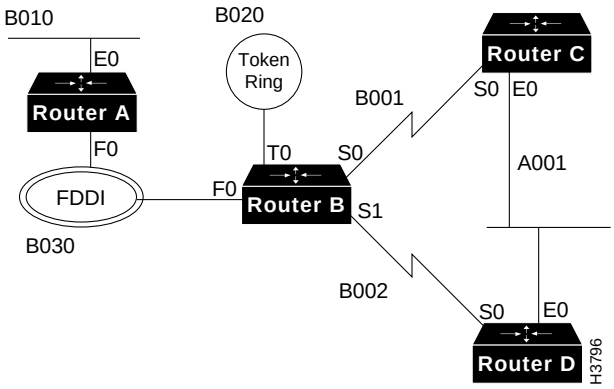
Internetwork Packet Exchange (IPX) is the Layer 3 protocol developed by Novell to deliver packets within a Novell internetwork.

The configuration command **ipx routing** is used to enable IPX routing on the Cisco IOS software.

IPX Network Numbering

IPX uses 32-bit network numbers to uniquely identify each data link in an IPX internetwork. An example Novell network numbering plan is shown in Figure A-12.

Figure A-12 IPX Network Numbering Plan



IPX Node Numbering

IPX uses a 48-bit address for the node. The IPX device will use the data link address of one interface as its IPX node address. Because the Layer 3 address is the same as the Layer 2 address, there is no need for an ARP process to perform network-to-data link layer address resolution.

IPX Routing Protocols

Cisco IOS software supports the following IPX routing protocols:

- IPX RIP
- IPX enhanced IGRP
- Novell Link State Protocol

IPX RIP is enabled by default. Enter the EXEC command **sh ipx route** to examine the IPX routing table in an access server running Cisco IOS software.

IPX Directory Services

Novell servers advertise their presence throughout the IPX internetwork with the Service Advertisement Protocol (SAP). Novell servers include file servers, print servers, and directory servers. Each type of server is advertised by a SAP type number as well as its IPX address.

SAP works like a distance vector routing protocol. Access servers and routers running IPX build server tables based on the SAPs they have received, and they advertise the servers they know to others with SAPs. Enter the command **show ipx servers** to see the server table in an access server running Cisco IOS software.

When an IPX client starts up, it sends a Get Nearest Server (GNS) request on its connected data link to locate the nearest Novell server. If there are no Novell servers on that data link, the access server responds with the best available server (based on cost) in its server table.

Cisco IOS software has many features to control SAP overhead and GNS functionality. No special configuration is required for standard SAP and GNS support.

IPX Data Link Encapsulations

Novell has defined four distinct encapsulations, or formats, for placing frames on a data link such as Ethernet. In order for two or more IPX devices on a data link to communicate, they must use the same encapsulation. Encapsulation on distinct data links do not have to agree in order to maintain connectivity. You must determine the encapsulation that will be used on each data link and network.

Table A-5 shows the four kinds of encapsulation available on Ethernet networks.

Table A-5 Ethernet Encapsulation Keywords

Novell Term	Cisco Term	Common Term
Ethernet_II	arpa	Ethernet
Ethernet_802.3	novell-ether	raw
Ethernet_802.2	sap	802.2
Ethernet_SNAP	snap	snap

For Novell NetWare 3.x and earlier versions, the default encapsulation was Ethernet_II. As of Netware 4.x, the default encapsulation is Ethernet_802.2.

In the example in Figure A-12, all Novell networks use SAP, or 802.2, except B010 which uses ARP for compatibility with older devices on the LAN links. These encapsulation issues do not apply to the WAN links.

IPX Configuration Example

The IPX configuration of Router C in Figure A-12 is as follows:

```
ipx routing
!
interface ethernet 0
ipx network A001 encapsulation sap
!
interface serial 0
ipx network B001
```

The IPX configuration of Router D in Figure A-12 is as follows:

```
ipx routing
!
interface ethernet 0
ipx network A001 encapsulation sap
!
interface serial 0
ipx network B002
```

AppleTalk Protocol

The AppleTalk protocol uses Datagram Delivery Protocol (DDP) at the network layer for addressing. Enter the configuration command **appletalk routing** to enable AppleTalk. Cisco IOS support of AppleTalk has extensive features and functionality that are not covered in this appendix.

AppleTalk Network Numbering

AppleTalk uses a 16-bit number to uniquely identify networks. There are two kinds of AppleTalk networks, extended and nonextended. Extended networks are used for all LANs and most WANs.

A single network number, such as 200, identifies a nonextended AppleTalk network. Nonextended networks can have a maximum of 253 nodes and a single zone name. See the section "AppleTalk Directory Services" later in this appendix for information on zones.

Nonextended networks are rarely used unless they are required for such support as a Phase 1 Ethernet (which is now obsolete), X.25, or LocalTalk.

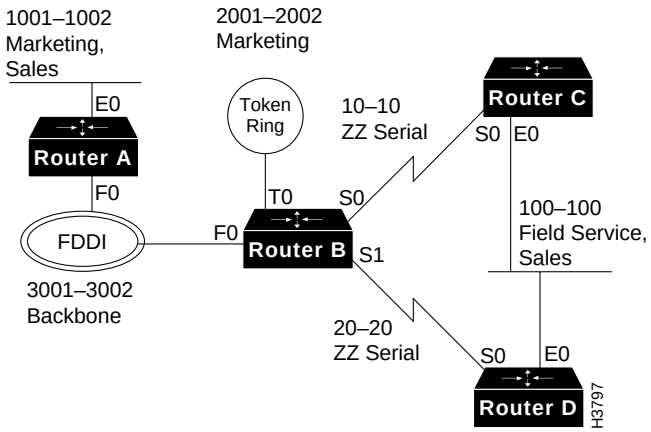
Extended networks allow a cable range that consists of one or more network numbers, such as 200-201, to be defined and used by nodes on that network.

The access server plays no role in routing packets between network numbers in a range as all the nodes know the full range of numbers that define the local data link.

Timesaver A good rule of thumb is to have one number in the range for every 50 AppleTalk devices on the LAN. For example, to support 300 devices, use a cable range of six (such as 201-206).

Figure A-13 shows a sample AppleTalk network numbering and zone naming plan. Zones are described in the section "AppleTalk Directory Services" later in this appendix.

Figure A-13 AppleTalk Numbering and Zone Naming Plan



AppleTalk Node Numbering

The AppleTalk node address is an eight-bit number. AppleTalk devices will dynamically find a free node address on startup using an extension of the AARP. You do not need to perform any node address adminstration.

When you are using dialer maps (for dial-on-demand routing) or some multipoint WAN data links, it is useful to tell the access server what node address to use. This can be done using an optional field on the **appletalk cable-range** command as follows:

```
appletalk cable-range 3-4 1.129
```

AARP is used to resolve network layer node addresses with data link addresses. Enter the command **show apple arp** to examine the AARP table.

AppleTalk Routing Protocols

Several AppleTalk routing protocols are available, including the following:

- Routing Table Maintenance Protocol (RTMP)
- AppleTalk Update Routing Protocol (AURP)
- Enhanced IGRP

The default AppleTalk routing protocol on the access server is RTMP. RTMP is a distance vector algorithm that advertises known extended and nonextended networks in the internetwork at ten-second intervals. AppleTalk nodes expect to see RTMP packets on the LAN in order to locate access servers and routers that are routing AppleTalk. Enter the command **show apple route** to examine the AppleTalk routing table.

AppleTalk Directory Services

AppleTalk directory services account for a significant portion of the functionality and usability of AppleTalk. AppleTalk directory services work as follows:

- Networks are assigned one or more zone names.
- Zones can appear on multiple networks.
- After an access server learns of a new route or network from its routing protocol, it will query the advertising router for the zones associated with that route (network).
- Each router builds a zone information table.
- When an AppleTalk node boots up, it uses the Get Net Info (GNI) routine to ask the AppleTalk routers on the network what zones are defined for that network. The node then selects one for itself that will be visible to other AppleTalk devices.

When an AppleTalk node needs directory services, it will ask a local access server or router routing AppleTalk to execute a lookup. For example, to find LaserWriters in the zone Marketing, the access server or router will create a packet destined for each network that has the zone Marketing assigned. Any device that matches this criterion will reply with its address. Once the device is selected and the address is obtained, the routing takes place on the network layer addresses, and the zone name is no longer involved in the connection.

In order to configure AppleTalk correctly, all AppleTalk access server or router interfaces on a data link must agree on the assigned cable range, default zone, and any additional zones. If there are any conflicts when a new router or access server using AppleTalk attempts to connect to the network, the interface will not enable AppleTalk and will report a port configuration mismatch. Enter the EXEC command **show apple interface** to confirm correct startup.

Zones should be named for ease of use. Zone names are logical and do not need to be unique, allowing logical groupings of users across diverse geographic locations. Because WAN links offer no AppleTalk services, you should name them to appear at the bottom of the Macintosh Chooser with a name such as "ZZ Serial."

For example, in Figure A-13, the following zone name assignments are used:

cable-range	default zone	additional zones
100–100	Field Service	Sales
1001–1002	Marketing	Sales
2001–2002	Marketing	
3001–3002	Backbone	
10–10	ZZ Serial	
20–20	ZZ Serial	

Using the zone name assignments above will cause each access server or router in the AppleTalk internetwork to build a zone information table that looks like this:

Marketing	1001–1002	2001–2002
Sales	1001–1002	100–100
Backbone	3001–3002	
Field Service	100-100	
ZZ Serial	10–10	20–20

Enter the command **show apple zone** to look at the zone information table of the access server or router.

When a node lookup request comes in for the zone Marketing, the device routing AppleTalk will create two packets for forwarding, one for network 1001–1002 and one for network 2001–2002.

AppleTalk Configuration Example

The AppleTalk configuration of Router C in Figure A-13 is as follows:

```
appletalk routing
!
interface ethernet 0
appletalk cable-range 100-100
appletalk zone Field Office
appletalk zone Sales
!
interface serial 0
appletalk cable-range 10-10
appletalk zone ZZ Serial
```

The AppleTalk configuration of Router D in Figure A-13 is as follows:

```
appletalk routing
!
interface ethernet 0
appletalk cable-range 100-100
appletalk zone Field Office
appletalk zone Sales
!
interface serial 0
appletalk cable-range 20-20
appletalk zone ZZ Serial
```

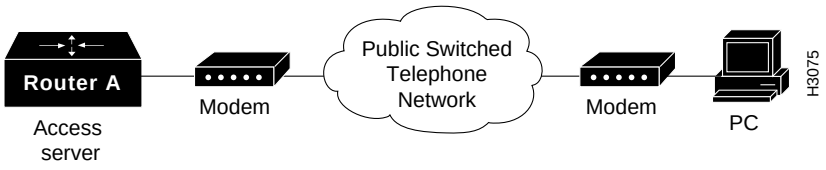
Modems

Modems are used with access servers to allow remote nodes and remote LANs to connect to internetworks across Public Switched Telephone Networks (PSTNs). (See Figure A-14.) This section contains the following sections:

- EIA/TIA-232 Standard and Cabling
- Configuring the Asynchronous Port
- Communicating with the Modem
- Configuring the Modem
- Testing the Dial-In Connection

Dialup access to an internetwork is achieved via modems connected to the asynchronous port of the access server. Before services such as remote node, remote LAN, and terminal services can be utilized by a remote device, the modem and access server must be configured to provide a reliable point-to-point WAN link. This section provides the background information the is required to resolve modem configuration issues, and step you through a modem setup.

Figure A-14 Connection Between an Access Server and a Modem



EIA/TIA-232 Standard and Cabling

This section discusses the EIA/TIA-232 implementation in detail as it applies to connecting the access server with the modem. On an EIA/TIA-232 connection between an access server and a modem, the access server is defined as data terminal equipment (DTE) and the modem is defined as data circuit-terminating equipment (DCE).

RJ-45 Cabling

The access server uses high-density, 68-pin connectors with an 8-connector breakout cable (with RJ-45 connectors) for its asynchronous ports. To connect to a modem, an MMOD type RJ-45-to-DB-25 adapter is used. The MMOD adapter is labelled "MODEM." (For connecting a modem on the auxiliary port, use an RJ-45 roll-over cable and an MMOD adapter.) For additional information about supported cabling configurations, see the appendix "Cable Specifications."

Note RJ-45 cabling for EIA/TIA-232 is not standardized and may vary if purchased from different vendors. The RJ-45-to-DB25 adapters modify the Cisco RJ-45 standard to the DB-25 standard.

EIA/TIA-232 Pairs

The EIA/TIA-232 cabling uses three pairs of wires (plus grounding) to connect the modem (DCE) to the access server (DTE). In each pair, one wire is used as output and one as input on each end. The three wire pairs are used for the following purposes:

- Data transfer (TX/RX)
- Hardware flow control (RTS/CTS)
- Modem control (DTR/DCD)

Table A-6 lists the signal flow between the two devices and their function for modem communications.

Table A-6 EIA/TIA-232 Signals and Functions

Signal Name	Asynchronous Port (DTE)	Modem (DCE)	Function
Transmit Data (TX)	Output	Input	DTE transmits data to DCE.
Receive Data (RX)	Input	Output	DCE transmits received data to DTE.
Request To Send (RTS)	Output	Input	DTE signals to DCE it can continue to accept data into its buffers.

Signal Name	Asynchronous Port (DTE)	Modem (DCE)	Function
Clear To Send (CTS)	Input	Output	DCE signals to DTE that it can continue to accept data into its buffers.
Data Terminal Ready (DTR)	Output	Input	DTE indicates to DCE that it can accept a call. Lowering and raising instructs DCE to drop the active call and return to the stored configuration.
Data Carrier Detect (DCD) (Connected to DSR input on access server.)	Input	Output	DCE indicates to DTE that a call is now present and established with a remote modem. Dropping DCD terminates the session.

Both the access server and the modem must be configured for correct operation on each of the pairs of wires. Understanding the configuration concerns for these signals simplifies modem setup and troubleshooting.

Data Transfer (TX/RX)

The data transfer wire pair is used for the transmission of user data (characters and packets) between the access server and the modem. The conditions that must be met when setting data transfer speeds are as follows:

- The access server asynchronous port and the modem must agree on the speed of data transfer used on this wire pair. (The modem must not change the speed on its EIA/TIA-232 port when a session is negotiated with a remote modem.)
- The speed used should take into account modulation speed (V.32 *bis*, V.34), compression ratio achieved (V.42 *bis*), and the length of the EIA/TIA-232 cables.

Hardware Flow Control (RTS/CTS)

Hardware flow control is used between the access server and the modem to start and stop data transfer on the TX/RX wire pair. Hardware flow control is used to prevent the loss of data when buffers are full. Hardware flow control is controlled on the RTS/CTS wire pair. The conditions that must be met when setting hardware flow control are as follows:

- Both the access server asynchronous port and the modem must be configured for hardware flow control.
- Software flow control must be turned off for packet data, because it can cause communications to stop unexpectedly.
- No flow control on either end will cause loss of data.

Modem Control (DTR/DCD)

Modem control is used between the access server and the modem to initiate and end calls. Modem control is performed on the DTR/DCD wire pair. The conditions that must be met when setting modem control are as follows:

- The modem should be configured so that if DTR is dropped and then raised, it will terminate any calls and return to its stored settings. This configuration is the standard for EIA/TIA-232 operations.
- The modem should be configured to only send the DCD signal to the access server when an active call has been negotiated and is established.

Configuring the Asynchronous Port

This section describes how to configure the Cisco 2500 series access server for use with a modem, and includes information on configuring the line and security commands.

Full configuration of an access server asynchronous port requires the configuration of two entities—the line and the asynchronous interface. The asynchronous interface is created and configured for support of Serial Line Internet Protocol (SLIP) and PPP. (See the section “Asynchronous Protocols” later in this appendix.)

Configuring the Line

The goal of line configuration is to prepare the line to test dial-in access to an EXEC session. In the following example, lines 1 through 8 are configured:

Step 1 From a privileged EXEC session, enter the command **configure terminal** and access line configuration mode:

```
Router# conf terminal
Enter one configuration command per line.  End with CNTL-Z.
Router(config)# line 1 8
Router(config-line)#
```

Step 2 Configure the lines to meet the EIA/TIA-232 requirements:

```
Router(config-line)# speed 57600
Router(config-line)# flowcontrol hardware
Router(config-line)# modem inout
Router(config-line)#
```

Setting the speed at 115200 may offer higher throughput depending on modem speed and compression achieved. Troubleshooting should include testing at lower speeds.

The command **modem ri-is-cd** can be used instead of the command **modem inout** to enhance security by not allow outgoing connections from the access server to the modem. Enter the command **modem inout** during setup to allow configuration of the modem from the access server, changing to the command **modem ri-is-cd** when testing is completed, if desired.

Security Commands

Security allows you to control access to the access server and its services. Each line should be configured with security. The following are some of the available security commands for protection of the EXEC sessions:

Global commands

The command **username** *name* **password** *password* is used for local login (using the command **loginlocal**), and protocol-specific (AppleTalk Remote Access (ARA), CHAP, and so forth) security.

Line security options

The **login tacacs** command allows for centralized and enhanced security with a Terminal Access Controller Access System (TACACS) server.

Use one of the login line subcommands from Table A-7 to control access to your EXEC session.

Table A-7 Login Line Subcommand Options

Line subcommand	Security Prompts	Function
no login	None	No security
login	Password:	Check the line subcommand **password**
login local	Username: Password:	Check the global username/password database in configuration mode
login tacacs	Username: Password:	Check the TACACS server[1]

1. See the publication *Access and Communication Server Configuration Guide* to set up TACACS support.

Configure security as follows:

```
Router(config)#username meredith password 123xyz
Router(config)#line 1 8
Router(config-line)#login local
```

With this configuration, the sign-on dialog from the remote PC appears as follows:

```
atdt5551234
CONNECT 14400/ARQ/V32/LAPM/V42BIS

User Access Verification

Username: meredith
Password:
Router>
```

Communicating with the Modem

You must establish communication with your modem before you can configure it, which requires terminal access to the modem's command environment. The access server's reverse Telnet feature is used to communicate with the modem. This section explains how to use reverse Telnet to access the modem.

Initiating a Reverse Telnet

To initiate a reverse Telnet, determine the IP address of your LAN (Ethernet) interface, then enter a Telnet command to port 2000 + *n* on the access server, where *n* is the line number for the modem to be configured. For example, to connect to the modem on line 1, enter the following command from an EXEC session on the access server:

```
Router# telnet 172.16.1.10 2001
Trying 172.16.1.10, 2001 ... Open
```

You can now communicate with the modem on line 1 using the **at** command set as defined by the modem vendor.

Timesaver Use the configuration command **ip host** to simplify reverse Telnets. For example, **ip host modem1 2001 172.16.1.10**.

If you are unable to connect to the modem, check the following:

1. The EXEC command **show users** should not indicate the line is in use.
2. The line should be configured for **modem inout**.
3. The output of the EXEC command **show line** *value* should contain the following two lines:

   ```
   Modem state: Idle
   Modem hardware state: CTS noDSR  DTR RTS
   ```

4. The line virtual terminal connections in the access server configuration may require passwords. See the publication *Troubleshooting Internetworks* for additional information on assigning passwords to virtual terminals.

Testing the Modem Connection

After connecting to the modem with a reverse Telnet, you need to test the connection. Send the modem the **at** command to request its attention. It should respond with OK:

```
at
OK
```

If the modem does not reply to the **at** command, check the following:

1. Look at the output of the command **show line 1**. If it displays "no CTS" for the modem hardware state, the modem is not connected, powered on, and waiting for data, or the modem might not be configured for hardware flow control.
2. You may have problems with your cabling or modem configuration (echo or result codes may be off). Try entering the command **at** to view the modem configuration, or entering the command **at&f** to return to factory defaults.

Initiating, Suspending, and Terminating Telnet Sessions

The reverse Telnet must be terminated before the line can accept incoming calls. If you don't terminate the session, it will be indicated in the output of the command **show users,** when it returns a modem state of ready if the line is still in use. If the line is no longer in use, the output of the command **show line** *value* will return a state of idle.

Terminating the Telnet session requires first suspending it, then disconnecting it. To suspend a Telnet session, enter the escape sequence **Ctrl-Shift-6-x**. You can then enter the EXEC command **disc** to terminate the telnet session.

Note Ensure that you can reliably issue the escape sequence to suspend a Telnet session. Some terminal emulator packages have difficulty sending the correct sequence, Ctrl-Shift-6-x.

An example of how to use reverse Telnet to communicate with a modem follows:

Step 1 Initiate the session:

```
Router#telnet 172.16.1.10 2001
Trying 172.16.1.10, 2001 ... Open
```

Step 2 Test Communications with the modem:

```
at
OK
```

Step 3 Suspend the Telnet session by entering **Ctrl-Shift-6-x**:

```
- suspend keystroke -
Router#
```

Step 4 Enter the EXEC command **where** to check for open sessions:

```
Router#where
Conn Host               Address             Byte  Idle Conn Name
*  1 172.16.1.10        172.16.1.10            0     0 172.16.1.10
```

Step 5 Enter the EXEC command **disc** to terminate the session:

```
Router#disc
Closing connection to 172.16.1.10 [confirm]y
Router#
```

After you have established and tested the connection to the modem, you can proceed with configuring the modem.

Configuring the Modem

A modem initialization string is a series of parameter settings that is sent to your modem to configure it for the desired operation. In this section, you will determine the correct initialization string for your modem and configure your modem with it.

Modem command sets vary widely. Although most modems use the Hayes command set (prefixing commands with **at**), Hayes-compatible modems do not use identical **at** command sets.

Refer to your modem manufacturer's documentation to learn how to examine the current and stored configuration of the modem you are using. Normally, you enter **at** commands such as **&v**, **i4**, or ***o** to view, inspect, or observe the settings.

Determine the Modem Initialization String

The initialization string is used to configure the modem for use. A sample modem initialization string for a US Robotics Courier modem would be as follows:

```
&b1&h1&r2&c1&d3&m4&k1s0=1
```

Timesaver Initialization strings for other modems are available from CIO.

Locking EIA/TIA-232 Speed

Lock the EIA/TIA-232 port speed of the modem to the port speed of the Cisco 2500 series access server. This speed must not change when a session is negotiated with a remote modem. If the speed of the port on the access server is changed, you must perform a reverse Telnet to the modem and send an **at** command for the modem to learn the new speed.

Modems differ in the method they use to lock the EIA/TIA-232 speed. In the modem documentation, vendors use terms such as, port-rate adjust, speed conversion, or buffered mode. Enabling error correction will often put the modem in the buffered mode. Refer to your modem documentation (check the settings **&b**, **\j**, **&q**, **\n**, or s-register settings).

Hardware Flow Control (RTS/CTS)

RTS and CTS must be used between the modem and the access server to control the flow of data. Misconfiguring flow control for software or setting no flow control, can result in hung sessions and loss of data.

Modems differ in the method they use to enable hardware flow control. Refer to your modem documentation (check the settings **\q**, **&e**, **&k**, **&h**, **&r**, or **s-register)**.

Correct DCD Operation

The modem must use the DCD wire to indicate to the access server when a session has been negotiated and is established with a remote modem. Most modems use the setting **&c1**. Refer to your modem documentation for the settings used with your modem.

Proper DTR Interpretation

The modem must interpret a toggle of the DTR signal as a command to drop any active call and return to the stored settings. Most modems use the settings **&d2** or **&d3**. Refer to your modem documentation for the settings used with your modem.

Other Modem Settings

This section defines other settings that may be needed or desirable depending on your modem. For these settings refer to your modem documentation.

Best error correction

Error correction can be negotiated between two modems to ensure a reliable data link. Error correction standards include LAPM and MNP4. V.42 error correction will allow either LAPM or MNP4 error correction to be negotiated.

Modems differ in the way they enable error correction. Refer to your modem documentation for the settings used with your modem.

Timesaver If you plan to support ARA v1.0 clients we suggest that you disable MNP4 error correction. Other users will negotiate LAPM.

Best data compression

Data compression can be negotiated between two modems and will allow for greater data throughput. Data compression standards include V.42 *bis* and MNP5.

Modems differ in the way they enable data compression. Refer to your modem documentation for the settings used with your modem.

Answering calls

If a modem will be used to service incoming calls, it must be configured to answer the phone after a specific number of rings.

Most modems use the setting s0=1 to answer the call after one ring. Refer to your modem documentation for the settings used with your modem.

Initializing the Modem

Once the modem initialization string has been determined, take the following steps to configure the modem. (This example configures a U.S. Robotics Courier modem on line 1):

Step 1 Reverse Telnet to the modem:

```
Router#telnet modem1
Trying modem1 (172.16.1.10, 2001)... Open
```

Step 2 Return the modem to its factory defaults (this step is optional):

```
at&f
OK
```

Step 3 Configure the modem with an initialization string:

```
at&b1&h1&r2&c1&d3&m4&k1s0=1
OK
```

Step 4 Store the modem settings in the modem NVRAM:

```
at&w
OK
```

Step 5 Suspend and disconnect your Telnet session:

```
- suspend keystroke -
Router#disc
Closing connection to modem1 [confirm]y
Router#
```

Timesaver The line configuration command **script-reset** can automate the configuration of your modems. See the publication *Access and Communication Servers Configuration Guide*, or the section "Tech Tips" on CIO for more information.

Testing the Dial-In Connection

The access server and modem are now correctly configured for dial-in access. Before configuring any additional protocols for the line (such as SLIP, PPP, or ARA), test the dial-in connection.

Note Remember, the same configuration issues exist between the client DTE (PC) and client modem. Make sure you have the correct EIA/TIA-232 cabling and modem initialization string for your client modem.

The following is an example of a successful connection from a PC using a U.S. Robotics Courier modem to dial into a Cisco 2500 series access server:

```
at&f&c1&d3&h1&r2&b1&m4&k1&w
OK
atdt9,5551234
CONNECT 14400/ARQ/V32/LAPM/V42BIS

User Access Verification

Username:
```

Asynchronous Protocols

The Cisco 2500 series access server supports a number of popular asynchronous protocols for remote node connectivity. This section provides background information and configuration guidance for accessing EXEC sessions and the asynchronous protocols PPP, SLIP, and ARA.

It is important to be familiar with the concepts EXEC, autoselect, lines, and asynchronous interfaces when you support asynchronous protocols.

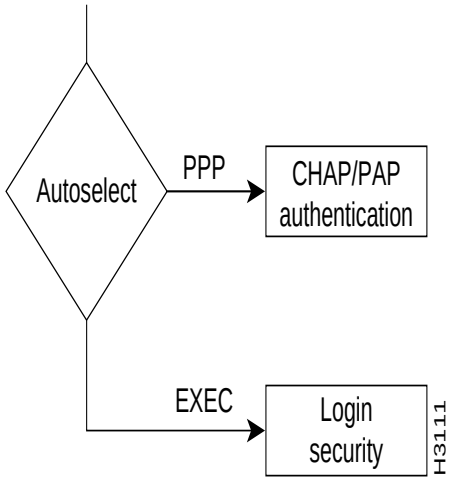
The EXEC Session

When a dial-in user connects to an asynchronous line on the access server, the session received after the security dialog is called an EXEC session. From an EXEC session, you can use terminal services (such as Telnet or rlogin), run an asynchronous protocol over the line, or use one of many other access server services. For example, you can enter the command **ppp** to initiate a PPP session.

Launching Autoselect

The access server can launch three asynchronous protocols (PPP, SLIP, or ARA) automatically if it detects that the remote device is using one of these protocols. The automatic detection of the asynchronous protocol is called autoselect. Autoselect will bypass the EXEC security dialog. If you use autoselect, we strongly recommend that you use the authentication techniques built into the asynchronous protocols. (See Figure A-15.)

Figure A-15 Flowchart for EXEC and AutoSelect Authentication Options



Configuring Asynchronous Ports

Cisco 2500 series access servers have 8 or 16 asynchronous ports (plus an asynchronous auxiliary port). These ports use RJ-45 connectors and the EIA/TIA-232 signaling standard. In the access server configuration, there are two configuration submodes associated with any asynchronous port—lines and asynchronous interfaces.

Asynchronous Lines

The line configuration subcommands are used to configure the asynchronous port for many options, including the following:

- Physical layer options
- EXEC security
- Autoselect
- ARA protocol

Asynchronous Interfaces

Asynchronous interfaces are created and configured in Cisco IOS software to support PPP and SLIP connections. The creation of an interface structure also allows Cisco IOS software to use routing functions on the lines as it would with other interfaces. To support SLIP or PPP on a given port, you must create and configure an asynchronous interface with the same number as the line. Typically, the asynchronous interface would be configured for the following features:

- Network protocol support (IP, IPX, or AppleTalk)
- Encapsulation support (PPP or SLIP)
- IP client addressing options (default and/or dynamic)
- IPX network addressing options
- PPP authentication (SLIP has no protocol security)

Modem Configuration

See the section “Modems” earlier in this appendix for assistance in configuring your access server and modem for proper operation. This section will involve configuring the line for EIA/TIA-232 options, and EXEC security.

Testing the Line for EXEC Functionality

Testing for access to EXEC functionality is a critical step in the configuration of the Cisco 2500 series access server ports. The successful access to an EXEC session can help ensure that the cabling, modem, and lines have correct configurations. A client should be able to connect to the line and receive a hostname> prompt. Further testing might include stress testing flow control and testing error correction.

Configuring PPP, SLIP, and ARA

The following sections discuss configuration options for PPP, SLIP and ARA

Point-to-Point Protocol

PPP allows a remote device to connect to the access server for multiple network (Layer 3) protocols simultaneously. For example, a PPP user could request IP, IPX, or Appletalk.

You configure PPP by configuring the asynchronous interface associated with the line.

In the following example, asynchronous port 1 is being configured for PPP. These steps are performed in configuration mode, as follows:

Step 1 Enter the following commands to create and configure the asynchronous interface for the line:

```
Router(config)#interface async 1
```

Step 2 Enable IP and IPX (or other protocols) by assigning network numbers. (IP can be configured by entering the command **ip unnumbered** rather than an IP subnet.) This example enables PPP to support IP control protocol (ipcp) and IPX control protocol (ipxcp). Enter the following interface subcommands to configure IP and IPX (use your administered IPX network number):

```
Router(config-if)#ip unnumbered ethernet 0
Router(config-if)#ipx network B011
```

Step 3 Define PPP (or SLIP) encapsulation as the default:

```
Router(config-if)#encapsulation ppp
```

Step 4 Enter the following command to allow the port to support services other than PPP (such as EXEC, SLIP, or ARA) (This step is optional):

```
Router(config-if)#async mode interactive
```

Step 5 Configure a default client IP address. This should be a valid, unique, and unused IP address for a subnet on a connected LAN:

```
Router(config-if)#async default ip address 172.16.1.12
```

You can also enter the following additional configuration commands:

asynchronous dynamic address (interface subcommand)	Allows you to dynamically select your own IP address when dialing in. Use caution to ensure that only valid IP addresses are used by the client.
ip tcp header compression passive (interface subcommand)	Instructs the access server port to perform compression of TCP headers if requested by the client.
autoselect ppp (line subcommand)	Automatically launches a PPP session if the client starts sending PPP packets after the modems have connected. If you use autoselect, You should use PPP authentications to prevent unauthorized access.
ppp authen chap **ppp authen pap** (interface subcommand)	Use CHAP or PAP to authenticate PPP sessions. Recommended for use with autoselect.

Note For additional information on these commands, see the publication *Access Server Configuration Guide*.

Serial Line Internet Protocol

Serial line internet protocol (SLIP) is an older protocol that supports IP only. Configuring SLIP is similar to configuring PPP for IP. To support SLIP, follow the basic configuration for PPP in the previous section, and ensure that one or both of the following (interactive asynchronous mode or SLIP encapsulation) is configured:

```
async mode interactive
encapsulation slip
```

AppleTalk Remote Access Protocol

AppleTalk Remote Access Protocol (ARA protocol) is used by remote Macintoshes to connect to an AppleTalk network. The ARA Protocol can only be used for AppleTalk, and does not support routing. The ARA protocol performs as a single-node bridge for connecting a single Macintosh to a remote network.

The ARA protocol is configured with global and line commands only. The ARA protocol does not use any asynchronous interface configuration.

A typical configuration for the ARA protocol would look as follows:

```
arap network 100 ARA Dialin
username xx password yy
!
line 1
arap enable
arap noguest
autoselect arap
```

The nonextended AppleTalk network number used with the command **arap network** must be unique within the AppleTalk internetwork.

ARA Authentication

You can use the line configuration command **autoselect arap** to launch ARA protocol automatically. The person logging into an access server that is using the ARA protocol, is authenticated against either the username and password database in the configuration of the access server, or against a TACACS server. To store the ARA protocol username database on a TACACS server may require that the tacacs server be enabled with the supplementary file. The following line command and the tacacs commands are entered to enable the supplementary file:

```
arap use-tacacs (single-line)
```

ARA and Error Correction

The ARA protocol negotiates MNP4 error correction between the two ARA devices (remote ARA client and Cisco IOS). MNP4 requires special support considerations for ARA v1.0 clients. Turning off MNP4 support on the access server modem can eliminate this problem. Refer to the publication *ARA Setup and Troubleshooting* which is available on CIO for additional information.

Configuration Example

The following is an example of asynchronous protocol configuration. In this example, the access server is configured to allow dial-in clients to launch ARA, SLIP, and PPP on line 1. All the connected modems are U.S. Robotics V.34 Courier modems.

```
hostname cs
!
appletalk routing
ipx routing
arap network 100 ARA Dialin
!
username Meredith password 7 ASD@#$ASD
chat-script usrv34 at&f1&D2SO=1
!
interface ethernet 0
ip address 172.16.1.10 255.255.255.0
ipx network B010
appletalk cable-range 1001-1002
appletalk zone Marketing
appletalk zone Sales
```

```
!
interface asynchronous 1
ip unnumbered ethernet 0
ipx network B011
encapsulation ppp
ip tcp header compression passive
asynchronous mode interactive
asynchronous default ip address 172.16.10.101
!
!
line 1 16
login local
modem inout
flow hardware
speed 115200
arap enable
arap noguest
autoselect arap
reset-script usrv34
```

APPENDIX B

Maintaining the Cisco 2500 Series Access Server

This appendix contains information about maintenance procedures you might need to perform on the Cisco 2500 series access server as your internetworking needs change. If any upgrades requiring hardware or software replacement are necessary, a related publication called a configuration note will ship to you automatically with the parts.

This appendix contains the following sections:

- Opening the Chassis
- Upgrading the Boot PROMs
- Installing Primary-Memory DRAM SIMMs
- Replacing System-Code SIMMs
- Closing the Chassis
- Recovering a Lost Enable Password
- Virtual Configuration Register Settings

Caution Before opening the chassis, ensure that you have discharged all static electricity from your body and be sure the power is off. Before performing any procedures described in this appendix, review the sections “Safety Recommendations,” “Maintaining Safety with Electricity,” “Preventing Electrostatic Discharge Damage,” and “General Site Requirements” in the chapter “Preparing to Install the Cisco 2500 Series Access Server.”

Warning Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units. (To see translated versions of this warning, refer to the appendix “Translated Safety Warnings.”)

Opening the Chassis

This section describes the procedure for opening the chassis by removing the chassis cover.

Warning Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected. (To see translated versions of this warning, refer to the appendix "Translated Safety Warnings.")

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity. (To see translated versions of this warning, refer to the appendix "Translated Safety Warnings.")

Tools Required

The following are the tools you will need to open the chassis:

- Medium-size flat-blade screwdriver (1/4 inch [0.625 cm])
- Size M 3.5 (metric) hex-head nut driver (optional)

Removing the Cover

You must open the access server chassis to gain access to its interior components: the system card, system code single inline memory modules (SIMMs), and dynamic random access memory (DRAM) SIMMs. Following are the steps required to remove the chassis cover. When opening the chassis, use Parts A and B in Figure B-1 as guides.

Step 1 Turn OFF the power but, to channel electrostatic discharge (ESD) voltages to ground, do not unplug the power cable.

Step 2 Remove all interface cables from the rear panel of the access server.

Step 3 Turn the unit upside down so that the top of the chassis is resting on a flat surface, and the front of the chassis is toward you. (See Figure B-1, Part A.)

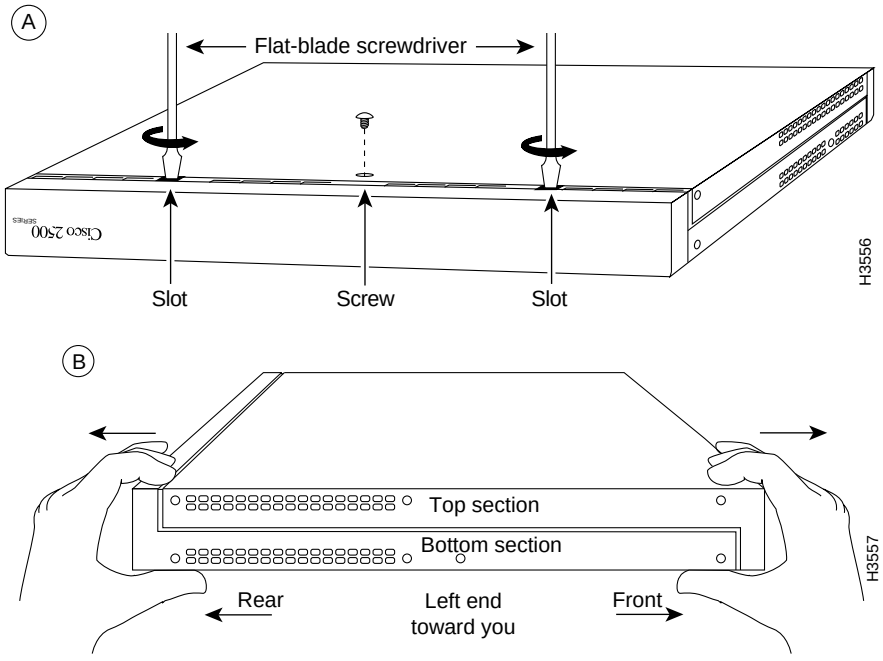
Step 4 Remove the single screw located on the bottom of the chassis (on the chassis side closest to you). Note that the chassis is comprised of two sections: top and bottom.

Step 5 If required, insert a medium-size flat-blade screwdriver into the slots shown in Figure B-1, Part A, and gently rotate the blade so that the top and bottom sections separate slightly.

Step 6 Holding the chassis with both hands, position it as shown in Figure B-1, Part B.

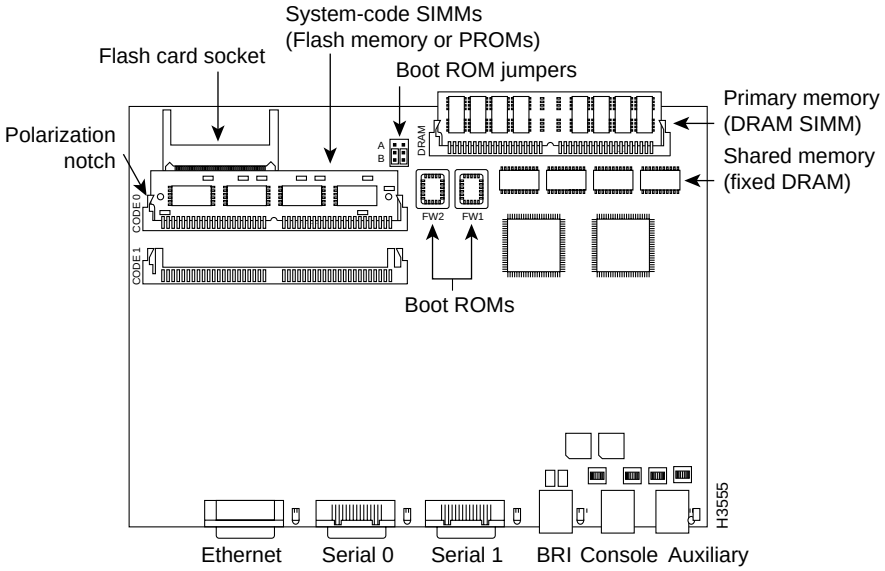
Step 7 Gently pull the top section away from the bottom section. (See Figure B-1, Part B.) The fit is very snug, so it may be necessary to work the chassis sections apart at one end and then the other, working back and forth.

Figure B-1 Chassis Cover Removal



Step 8 When the top cover is off, set it aside. Figure B-2 shows the layout of the system card, which is attached to the bottom section of the chassis.

Figure B-2 System Card Layout—Model 2509



Upgrading the Boot PROMs

To replace the boot programmable read only memory (PROM) software with a new software image, you need to replace the existing boot PROMs. Table B-1 lists the part numbers you need and indicates their installation socket. The part number is printed on a label attached to the boot PROM.

Table B-1 Boot PROM Part Numbers and Installation Sockets

Boot PROM Part Number	Installation Socket
17-1610-03	FW1
17-1611-03	FW2

Tools and Equipment Required for Replacing the Boot PROMs

The following tools and equipment are required to replace the boot PROMs:

- Erasable programmable read-only memory (EPROM) extraction tool or a small flat-blade screwdriver
- Two boot PROMs

Replacing the Boot PROMs

Take the following steps to replace the boot PROMs:

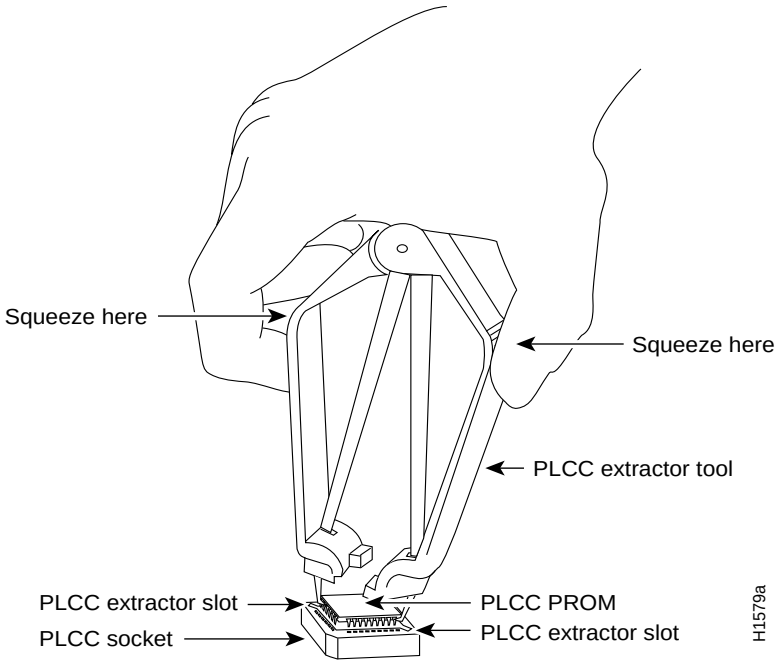
Step 1 To open the chassis and expose the boot PROMs, follow the procedures in the section "Opening the Chassis" earlier in this appendix.

Step 2 Locate the boot PROMs FW1 and FW2 (see Figure B-2).

Caution The correct placement of the boot PROMs is crucial. If the PROMs are installed in the wrong sockets, they could be damaged when the system is powered on. To prevent damage to the PROMs from ESD (when handling the system and its components), follow the ESD procedures described in the section "Preventing Electrostatic Discharge Damage" in the chapter "Preparing to Install the Cisco 2500 Series Access Server." Also, be careful not to damage or scratch the printed circuit card under the PROMs.

Step 3 Using an EPROM extraction tool or a small flat-blade screwdriver, gently remove the boot PROMs (see Figure B-3) and set them aside on a nonconductive surface.

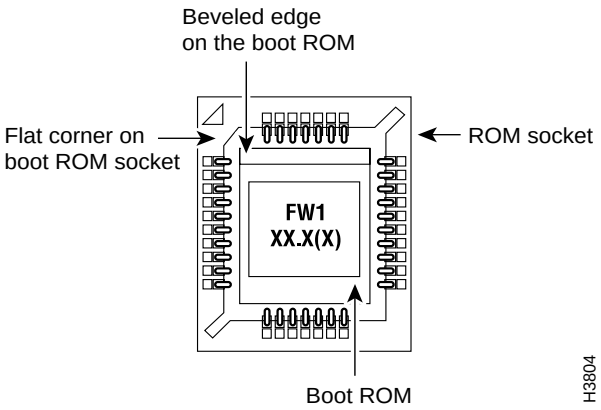
Figure B-3 Extracting and Inserting Boot PROMs



Step 4 Insert each new boot PROM in its socket in the orientation shown in Figure B-4. Insert the new boot ROMs in their respective sockets so that the beveled edge of the ROM chip is on the same side as the flat corner on the ROM socket.

Caution Boot PROMs should be installed with the printed label side up. Installing boot PROMs with the label side down will result in damage to the PROM (see Figure B-4).

Figure B-4 Orienting the Boot PROMs to the Socket



Step 5 Replace the tray assembly and cover following the instructions in the section "Closing the Chassis" later in this appendix.

Installing Primary-Memory DRAM SIMMs

The access server contains primary and shared (or packet) memory. Primary memory size, in kilobytes (KB), is displayed in the system banner on the console screen. Primary and shared memory are 1 MB each of the DRAM on the system card.

After booting up, your system will indicate in the system banner the amount of primary memory it has. The following example shows a system with 4 MB (4,096 KB) of primary memory. (The system does not display shared memory.)

```
System Bootstrap, Version 4.14(8), SOFTWARE
Copyright (c) 1986-1995 by Cisco Systems
2500 processor with 4096 Kbytes of main memory
```

If you use very large routing tables or many protocols, you might need to expand primary memory. This expansion might be necessary with configurations in which the access server is set up as a connection device between large external networks and your internal network.

Tools and Equipment Required

The following lists the tools required to remove and replace the DRAM SIMMs on the access server:

- Medium-size flat-blade screwdriver (1/4 inch [0.625 cm])
- ESD-preventive wrist strap
- The appropriate DRAM SIMM for your access server model

Primary Memory Configurations

You can upgrade to 4- or 16-MB DRAM; the 4-MB upgrade kit includes one 1 MB x 36 DRAM SIMM, and the 16 MB kit includes one 4 MB x 36 DRAM SIMM. As primary memory is expanded to 4- or 16-MB SIMMs, the 2 MB of permanent memory is allocated as shared memory.

DRAM SIMM Installation

Following is the procedure for installing DRAM SIMMs:

Step 1 Turn OFF power but, to channel ESD voltages to ground, do not unplug the power cord.

Step 2 Attach an ESD-preventive wrist strap.

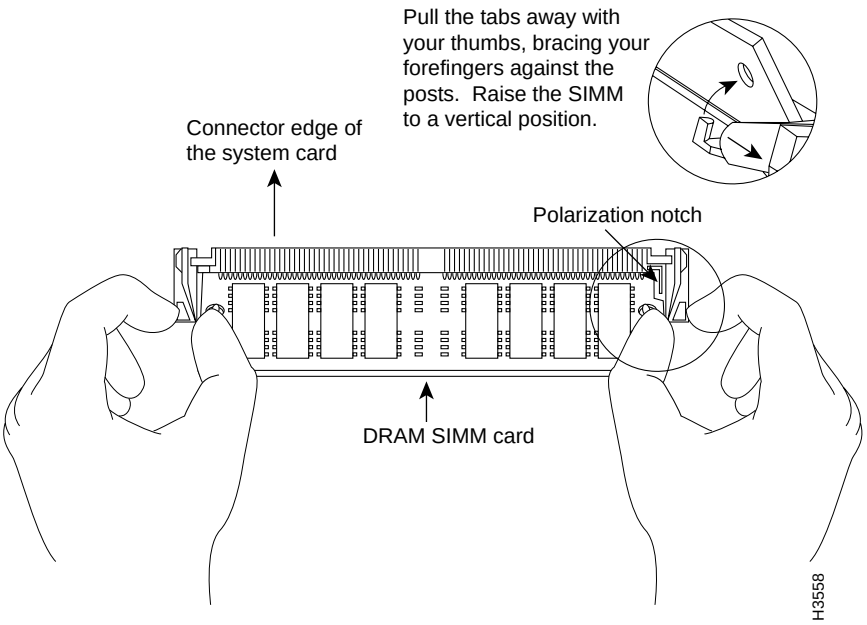
Step 3 Open the cover according to the procedure in the section “Opening the Chassis” earlier in this appendix.

Step 4 Turn the chassis so the system card is opposite the position shown in Figure B-2, with the primary-memory DRAM SIMM socket toward you.

Step 5 Remove the existing DRAM SIMM by pulling outward on the connectors to unlatch them, as shown in Figure B-5. Be careful not to break the holders on the SIMM connector.

Caution To prevent damage, do not press on the center of the SIMMs. Handle each SIMM carefully.

Figure B-5 Removing and Replacing the DRAM SIMM



Step 6 Using the system card orientation shown in Figure B-5, position the new SIMM so that the polarization notch is located at the right end of the SIMM socket. Note that the orientation of the system card is opposite that shown in Figure B-2.

Step 7 Insert the new DRAM SIMM by sliding the end with the metal fingers into the SIMM connector socket at approximately a 45-degree angle to the system card. Gently rock the SIMM back into place until the latch on either side snaps into place. Do not use excessive force because the connector could break.

Step 8 Replace the access server cover using the procedure in the section “Closing the Chassis” later in this appendix.

Step 9 Connect the access server to a console terminal.

Step 10 Turn on the power to the chassis. If error messages relating to memory are displayed, repeat these steps, taking care to firmly seat the SIMM in its socket.

Replacing System-Code SIMMs

The system code (software) is stored on Flash memory or PROM SIMMs. The 80-pin Flash memory and PROM SIMMs must be purchased from us. Contact a customer service representative for more information.

Note The system code for all the access server models can be contained on either one or two 80-pin Flash memory or PROM SIMMs. If only one 80-pin SIMM socket is populated, it must be the SIMM socket indicated in Figure B-2 (*CODE 0*).

Tools and Equipment Required

The following lists the tools required to remove and replace the system-code SIMMs on the access server:

- Medium-size flat-blade screwdriver (1/4 inch [0.625 cm])
- ESD-preventive wrist strap
- The appropriate system-code SIMM(s) for your access server model

  Flash memory and PROM SIMMs for the access server are available only from us. Contact a customer service representative for more information.

System-Code SIMM Replacement

Following is the procedure for upgrading the system-code Flash memory or PROM SIMMs:

Step 1 Turn OFF power but, to channel ESD voltages to ground, do not unplug the power cord.

Step 2 Attach an ESD-preventive wrist strap.

Step 3 Open the chassis cover using the tools and procedures in the section “Opening the Chassis” earlier in this appendix.

Step 4 Turn the chassis so that the system card is opposite the position shown in Figure B-2, with the system-code SIMMs toward you.

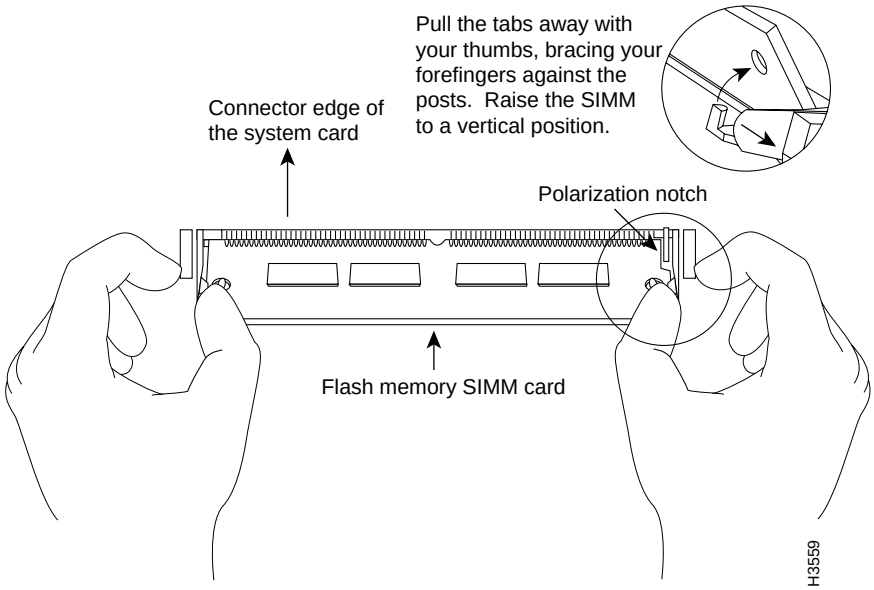
Step 5 Locate the system-code SIMMs on the system card. The SIMM sockets are labeled *CODE 0* and *CODE 1* (shown in Figure B-2).

Step 6 Remove the existing system-code SIMM by pulling outward on the connector holders to unlatch them. The connector holds the SIMM tightly, so be careful not to break the holders on the SIMM connector. (See Figure B-6.)

Caution To prevent damage, do not press on the center of the SIMMs. Handle each SIMM carefully.

Step 7 Repeat these steps for all the system-code SIMMs to be replaced.

Figure B-6 Removing and Replacing the System-Code SIMM



Step 8 Using the system card orientation shown in Figure B-6, position the new SIMM so that the polarization notch is located at the right end of the SIMM socket. Note that the orientation of the system card is the opposite of that shown in Figure B-2.

Caution To prevent damage, note that some Flash SIMMs have the components mounted on the rear side; therefore, when inserting the SIMM, always use the polarization notch as a reference and *not* the position of the components on the SIMM.

Step 9 Insert the new SIMM by sliding the end with the metal fingers into the appropriate SIMM connector socket (*CODE 0* or *CODE 1* shown in Figure B-2) at approximately a 45-degree angle to the system card. Gently rock the SIMM back into place until the latch on either side snaps into place. Do not use excessive force because the connector could break.

Step 10 Replace the access server cover using the procedure in the following section, "Closing the Chassis."

Step 11 Connect the access server to a console terminal.

Step 12 Turn on the power to the chassis.

If error messages relating to memory display, repeat these Steps, taking care to firmly seat the SIMM in the socket.

Closing the Chassis

This section describes the procedure for closing the chassis.

Tools Required

Following are the tools required for replacing the cover:

- Medium-size flat-blade screwdriver (1/4 inch [0.625 cm])
- Size M 3.5 hex-head nut driver (optional)

Replacing the Cover

After you perform the maintenance for your system, take the following steps to replace the cover:

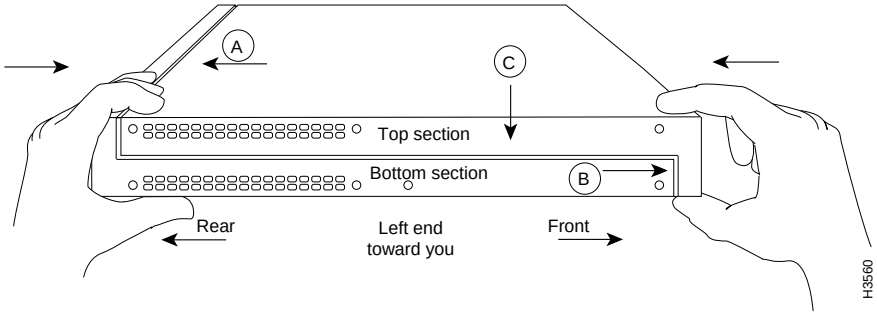
Step 1 Position the two chassis sections as shown in Figure B-7.

Step 2 Referring to Figure B-7, press the two chassis sections together and ensure the following:

- The top section fits *into* the rear of the bottom section. (See A in Figure B-7.)
- The bottom section fits *into* the front of the top section. (See B in Figure B-7.)
- Each side of the top and bottom sections fits together. (See C in Figure B-7.)

Caution To fit the two sections together, it may be necessary to work them together at one end and then the other, working back and forth; however, use care to prevent bending of the chassis edges.

Figure B-7 Replacing the Chassis Cover



Step 3 When the two sections fit together snugly, turn the chassis so that the bottom is facing up, with the front panel toward you.

Step 4 Replace the cover screw. Tighten the screw to no more than 8 or 9 inch/pounds of torque.

Step 5 Reinstall the chassis on the wall, rack, desktop, or table.

Step 6 Replace all cables.

Recovering a Lost Enable Password

This section describes in outline and then in detail how to recover a lost enable password.

Note Recovering a lost password is possible on the enable password. Systems running Cisco IOS Release 10.3(2) or later use the enable secret password, which is encrypted and must be replaced with a new enable secret. See the section "Hot Tips" on CIO for information on replacing enable secret passwords.

- Enter the command **show version** to note the existing virtual configuration register value.
- Break to the bootstrap program prompt (ROM monitor). This will require a reload of the image.
- Change the configuration register to 0x142 (ignore break; ignore NVRAM; boot from Flash memory).

Note A key to recovering a lost enable password is to set the configuration register so that the contents of NVRAM are ignored (0x0040), allowing you to see your password.

- Enter privileged mode in the system bootstrap program.
- Enter the command **show configuration** to display the enable password.
- Change the configuration register value back to its original setting.

Note To recover a lost enable password if Break is disabled on the router, you must have physical access to the access server.

Take the following steps to recover a lost enable password:

Step 1 Attach an ASCII terminal to the access server console port, which is located on the rear panel.

Step 2 Configure the terminal to operate at 9600 baud, 8 data bits, no parity, 2 stop bits.

Step 3 Enter the command **show version** to display the existing configuration register value.

Step 4 If Break is disabled, power cycle the access server. (Turn the access server off, wait five seconds, and then turn it on again.) If Break is enabled on the access server, send a Break and then proceed to Step 6.

Step 5 Within 60 seconds of turning on the access server, press the Break key. This action causes the terminal to display the bootstrap program prompt (>).

Step 6 To reset the configuration register to boot from the boot ROMs and ignore NVRAM, enter **o/r** at the bootstrap prompt as follows:

```
> o/r 0x042
```

Step 7 Initialize the access server by entering the command **initialize** as follows:

```
> i
```

The access server will power cycle; the configuration register will be set to 0x142; and the access server will boot the boot ROM system image and prompt you with the system configuration dialog as follows:

```
--- System Configuration Dialog ---
```

Step 8 Enter **no** in response to the system configuration dialog prompts until the following system message is displayed:

```
Press RETURN to get started!
```

Step 9 Press **Return**. The boot ROM prompt appears as follows:

```
Router>
```

Step 10 Enter the **enable** command to enter the EXEC mode in the boot ROM image. Then enter the command **configure memory** as follows:

```
Router# configure memory
```

Step 11 Enter the EXEC command **configure terminal** to display the enable password in the configuration file and to display any boot system commands.

```
Router# configure terminal
```

Step 12 Enter the new passwords:

```
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.

  Enter enable secret : shovel

The enable password is used when there is no enable secret
and when using older software and some boot images.

  Enter enable password : trowel
```

Step 13 Set the configuration register to boot from Flash memory and to ignore the break key:

```
config-reg 0x2102
```

Step 14 Exit configuration mode by pressing **Ctrl-Z**.

Step 15 Reboot the access server and enter the recovered password.

Virtual Configuration Register Settings

The access server has a 16-bit virtual configuration register, which is written into NVRAM. You might want to change the virtual configuration register settings for the following reasons:

- Set and display the configuration register value
- Force the system into the ROM monitor or boot ROM.
- Select a boot source and default boot filename
- Enable or disable the Break function
- Control broadcast addresses
- Set the console terminal baud rate
- Recover a lost password (ignore the NVRAM startup-config)
- Enable booting from a Trivial File Transfer Protocol (TFTP) server

Table B-2 lists the meaning of each of the virtual configuration memory bits and defines the boot field names.

Caution To avoid confusion and possibly halting the access server, remember that valid configuration register settings might be combinations of settings and not just the individual settings listed in Table B-2. For example, the factory default value of 0x2102 is a combination of settings.

Table B-2 Virtual Configuration Register Bit Meanings

Bit No.[1]	Hexadecimal	Meaning
00–03	0x0000–0x000F	Boot field
06	0x0040	Causes system software to ignore the contents of NVRAM (startup-config)
07	0x0080	OEM bit is enabled
08	0x0100	Break is disabled
10	0x0400	IP broadcast with all zeros

Bit No.[1]	Hexadecimal	Meaning
11–12	0x0800–0x1000	Console line speed
13	0x2000	Load the boot ROM software if a Flash boot fails five times
14	0x4000	IP broadcasts do not have network numbers
15	0x8000	Enable diagnostic messages and ignore the contents of NVRAM

1. The factory default value for the configuration register is 0x2102. This value is a combination of the following: bit 13 = 0x2000, bit 8 = 0x0100, and bits 00 through 03 = 0x0002.

Changing Configuration Register Settings

You might want to modify the value of the virtual configuration register for the following reasons:

- Recover a lost password.
- Change the console baud rate.
- Enable or disable Break.
- Allow you to manually boot the operating system using the **b** command at the bootstrap program (ROM monitor) prompt.
- Force the access server to boot automatically from the system bootstrap software (boot ROM image) or from its system image in Flash memory, and read any **boot system** commands that are stored in the configuration file in NVRAM. If the access server finds no **boot system** commands, it uses the configuration register value to form a filename from which to boot a default system image stored on a network server.

To change the configuration register while running the system software, take the following steps:

Step 1 Enter the **enable** command and your password to enter privileged mode:

```
router> enable
Password:
router#
```

Step 2 At the privileged-level system prompt (access server #), enter the command **configure terminal.** You will be prompted as shown in the following example:

```
router# conf term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
```

Step 3 To set the contents of the configuration register, enter the configuration command **config-register** *value* where *value* is a hexadecimal number preceded by 0x (see Table B-2 and Table B-3):

config-register 0x*value*

(The virtual configuration register is stored in NVRAM.)

Table B-3 Explanation of Boot Field (Configuration Register Bits 00 to 03)

Boot Field	Boot Process
0x0	Stops the boot process in the ROM monitor
0x1	Stops the boot process in the boot ROM monitor
0x3–0xF	Specifies a default filename for booting over the network from a TFTP server Enables boot system commands that override the default filename for booting over the network from a TFTP server
0x2	Full boot process, load Cisco IOS software in Flash memory

Step 4 Exit configuration mode by pressing **Ctrl-Z**. The new settings will be saved to memory; however, the new settings do not take effect until the system software is reloaded by rebooting the access server.

Step 5 To display the configuration register value currently in effect and the value that will be used at the next reload, enter the EXEC command **show version**. The value will be displayed on the last line of the screen display:

```
Configuration register is 0x142 (will be 0x102 at next reload)
```

Step 6 Reboot the access server. The new value takes effect. Configuration register changes take effect only when the server restarts, which occurs when you switch the power off and on or when you issue a **reload** command from the console.

Virtual Configuration Register Bit Meanings

The lowest four bits of the virtual configuration register (bits 3, 2, 1, and 0) form the boot field. (See Table B-3.) The boot field specifies a number in binary form. If you set the boot field value to 0, you must boot the operating system manually by entering the **b** command at the bootstrap prompt, as follows:

```
> b [tftp] flash filename
```

The **b** command options are as follows:

- **b**—Boots the default system software from ROM
- **b flash**—Boots the first file in Flash memory
- **b** *filename [host]*—boots from the network using a TFTP server
- **b flash** *[filename]*—Boots the file *filename* from Flash memory

For more information about the command **b [tftp] flash** *filename*, refer to the publication *Router Products Configuration Guide*.

If you set the boot field value to a value of 0x2 through 0xF, and there is a valid system boot command stored in the configuration file, then the access server boots the system software as directed by that value. If you set the boot field to any other bit pattern, the access server uses the resulting number to form a default boot filename for booting from the network using a TFTP server. (See Table B-4.)

Table B-4 Default Boot Filenames

Action or Filename	Bit 3	Bit 2	Bit 1	Bit 0
bootstrap mode	0	0	0	0
ROM software	0	0	0	1
cisco2-igs	0	0	1	0
cisco3-igs	0	0	1	1

Action or Filename	Bit 3	Bit 2	Bit 1	Bit 0
cisco4-igs	0	1	0	0
cisco5-igs	0	1	0	1
cisco6-igs	0	1	1	0
cisco7-igs	0	1	1	1
cisco10-igs	1	0	0	0
cisco11-igs	1	0	0	1
cisco12-igs	1	0	1	0
cisco13-igs	1	0	1	1
cisco14-igs	1	1	0	0
cisco15-igs	1	1	0	1
cisco16-igs	1	1	1	0
cisco17-igs	1	1	1	1

In the following example, the virtual configuration register is set to boot the access server from Flash memory and to ignore Break at the next reboot of the access server:

```
router# conf term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
config-register 0x102
boot system flash [filename]
^Z
router#
```

The server creates a default boot filename as part of the automatic configuration processes. To form the boot filename, the server starts with *cisco* and links the octal equivalent of the boot field number, a dash, and the processor-type name.

Note A **boot system** configuration command in the access server configuration in NVRAM overrides the default boot filename.

Bit 8 controls the console Break key. Setting bit 8 (the factory default) causes the processor to ignore the console Break key. Clearing bit 8 causes the processor to interpret the Break key as a command to force the system into the bootstrap monitor, thereby halting normal operation. A break can be sent in the first 60 seconds while the system reboots, regardless of the configuration settings.

Bit 10 controls the host portion of the IP broadcast address. Setting bit 10 causes the processor to use all zeros; clearing bit 10 (the factory default) causes the processor to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the broadcast address. (See Table B-5.)

Table B-5 Configuration Register Settings for Broadcast Address Destination

Bit 14	Bit 10	Address (<net> <host>)
Off	Off	<ones> <ones>
Off	On	<zeros> <zeros>
On	On	<net> <zeros>
On	Off	<net> <ones>

Bits 11 and 12 in the configuration register determine the baud rate of the console terminal. Table B-6 shows the bit settings for the four available baud rates. (The factory-set default baud rate is 9600.)

Table B-6 System Console Terminal Baud Rate Settings

Baud	Bit 12	Bit 11
9600	0	0
4800	0	1
1200	1	0
2400	1	1

Bit 13 determines the server response to a bootload failure. Setting bit 13 causes the server to load operating software from ROM after five unsuccessful attempts to load a boot file from the network. Clearing bit 13 causes the server to continue attempting to load a boot file from the network indefinitely. By factory default, bit 13 is set to 1.

Enabling Booting from Flash Memory

To disable break and enable the **boot system flash** command, enter the **config-register** command with the value shown in the following example:

```
router# config term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
config-reg 0x2102
^Z
router#
```

Copying to Flash Memory

Copying a new image to Flash memory might be required whenever a new image or maintenance release becomes available. To copy a new image into Flash memory (write to Flash), you *must* first reboot from ROM and *then* copy the new image into Flash memory. You *cannot* copy a new image into Flash memory while the system is running from Flash memory. Use the **copy tftp flash** command for the copy procedure.

Following is the sample output for reloading the access server and then copying a file (called *IJ09140Z*) to Flash memory from a TFTP server (called *server1*):

```
router# configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
config-reg 0x2101
^Z
```

The configuration register setting 0x2101 tells the system to boot from ROM, but does *not* reset the break disable or check for a default netboot filename.

```
router# reload
...
router(boot)# copy tftp flash
```

```
IP address or name of remote host [255.255.255.255]? server1
Name of tftp filename to copy into flash []? IJ09140Z
copy IJ09140Z from 131.131.101.101 into flash memory? [confirm] <Return>
xxxxxxxx bytes available for writing without erasure.
erase flash before writing? [confirm] <Return>
Clearing and initializing flash memory (please wait)####...
Loading from 101.2.13.110: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!... [OK - 324572/524212 bytes]
Verifying checksum...
VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
VVVVVVV...
Flash verification successful. Length = 1204637, checksum = 0x95D9

router(boot)# config term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
config-reg 0x2102
^Z
```

The configuration register setting 0x2102 tells the system to boot from ROM if netboot fails, disable break, and check for a default netboot filename.

```
router(boot)# reload
...
```

The system is now ready to be configured to boot from the new image you copied to Flash memory. For more information on the **copy tftp flash** command and other related commands, refer to the publication *Access and Communication Servers Configuration Guide*.

APPENDIX C

Cable Specifications

This appendix provides the following pinout information:

- Console Port Pinouts (RJ-45), Table C-1
- Auxiliary Port Pinouts (RJ-45), Table C-2
- EIA-530 DTE Cable Pinout (DB-60 to DB-25), Table C-3
- EIA/TIA-232 DTE Cable Pinout (DB-60 to DB-25), Table C-4
- EIA/TIA-232 DCE Cable Pinout (DB-60 to DB-25), Table C-5
- EIA/TIA-449 DTE Cable Pinout (DB-60 to DB-37), Table C-6
- EIA/TIA-449 DCE Cable Pinout (DB-60 to DB-37), Table C-7
- V.35 DTE Cable Pinout (DB-60 to 34-Pin), Table C-8
- V.35 DCE Cable Pinout (DB-60 to 34-Pin), Table C-9
- X.21 DTE Cable Pinout (DB-60 to DB-15), Table C-10
- X.21 DCE Cable Pinout (DB-60 to DB-15), Table C-11
- Ethernet (AUI) Cable Pinout (DB-15), Table C-12
- Token Ring Port Pinout (DB-9), Table C-13
- Asynchronous Breakout Cable Pinout (8-Pin RJ-45), Table C-14
- Asynchronous-Line Cable Pinout (68-Pin SCSI), Table C-15
- Pinouts for the RJ-45-to-DB-25 Adapters, Table C-16
- Asynchronous Device Cabling Options, Table C-17

Console and Auxiliary Port Signals and Pinouts

The console port is configured as data communications equipment (DCE), and the auxiliary port is configured as data terminal equipment (DTE). The console and auxiliary ports both use RJ-45 connectors. RJ-45-to-DB-25 adapters are available for connection to modems and other external communications equipment. Both ports are configured as asynchronous serial ports.

Following are the pinouts for the console port (see Table C-1), the auxiliary port (see Table C-2), and the adapter (see Table C-16 and Table C-17).

Table C-1 Console Port Pinouts (RJ-45)

Console Port (DTE)		
Pin[1]	**Signal**	**Input/Output**
1	–	–
2	DTR	Output
3	TxD	Output
4	GND	–
5	GND	–
6	RxD	Input
7	DSR	Input
8	–	–

1. Any pin not referenced is not connected.

Table C-2 Auxiliary Port Pinouts (RJ-45)

Auxiliary Port (DTE)		
Pin[1]	**Signal**	**Input/Output**
1	RTS	Output
2	DTR	Output
3	TXD	Output

Auxiliary Port (DTE)		
Pin[1]	**Signal**	**Input/Output**
4	GND	–
5	GND	–
6	RXD	Input
7	DSR	Input
8	CTS	Input

1. Any pin not referenced is not connected.

Serial Cable Assemblies and Pinouts

The following illustrations and tables provide assembly drawings and pinouts for the EIA-530 DCE, and EIA/TIA-232, EIA/TIA-449, V.35, and X.21 DTE and DCE cables.

EIA-530

Figure C-1 shows the EIA-530 serial cable assembly, and Table C-3 lists the pinouts. Arrows indicate signal direction: —> indicates DTE to DCE, and <— indicates DCE to DTE.

Figure C-1 EIA-530 Serial Cable Assembly

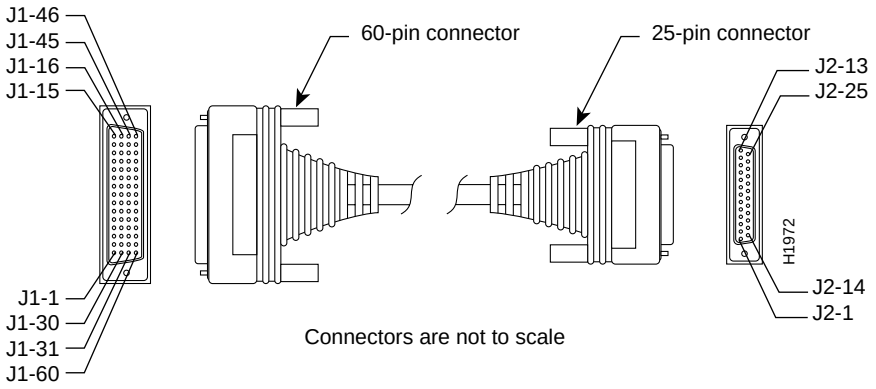


Table C-3 EIA-530 DTE Cable Pinout (DB-60 to DB-25)

60 Pin[1]	Signal	25 Pin	Signal	Direction DTE DCE[2]
J1-11	TxD/RxD+	J2-2	BA(A), TxD+	—>
J1-12	TxD/RxD–	J2-14	BA(B), TxD–	—>
J1-28	RxD/TxD+	J2-3	BB(A), RxD+	<—
J1-27	RxD/TxD–	J2-16	BB(B), RxD–	<—
J1-9	RTS/CTS+	J2-4	CA(A), RTS+	—>
J1-10	RTS/CTS–	J2-19	CA(B), RTS–	—>
J1-1	CTS/RTS+	J2-5	CB(A), CTS+	<—
J1-2	CTS/RTS–	J2-13	CB(B), CTS–	<—
J1-3	DSR/DTR+	J2-6	CC(A), DSR+	<—
J1-4	DSR/DTR–	J2-22	CC(B), DSR–	<—
J1-46	Shield_GND	J2-1	Shield	Shorted
J1-47	MODE_2	–	–	
J1-48	GND	–	–	Shorted
J1-49	MODE_1	–	–	

60 Pin[1]	Signal	25 Pin	Signal	Direction DTE DCE[2]
J1-5	DCD/DCD+	J2-8	CF(A), DCD+	<—
J1-6	DCD/DCD–	J2-10	CF(B), DCD–	<—
J1-24	TxC/RxC+	J2-15	DB(A), TxC+	<—
J1-23	TxC/RxC–	J2-12	DB(B), TxC–	<—
J1-26	RxC/TxCE+	J2-17	DD(A), RxC+	<—
J1-25	RxC/TxCE–	J2-9	DD(B), RxC–	<—
J1-44	LL/DCD	J2-18	LL	—>
J1-45	Circuit_GND	J2-7	Circuit_ GND	–
J1-7	DTR/DSR+	J2-20	CD(A), DTR+	—>
J1-8	DTR/DSR–	J2-23	CD(B), DTR–	—>
J1-13	TxCE/TxC+	J2-24	DA(A), TxCE+	—>
J1-14	TxCE/TxC–	J2-11	DA(B), TxCE–	—>

1. Any pin not referenced is not connected.
2. The EIA-530 interface cannot be operated in DCE mode. A DCE cable is not available for the EIA-530 interface.

EIA/TIA-232

Figure C-2 shows the EIA/TIA-232 cable assembly; Table C-4 lists the DTE pinout; and Table C-5 lists the DCE pinout. Arrows indicate signal direction: —> indicates DTE to DCE, and <— indicates DCE to DTE.

Figure C-2 EIA/TIA-232 Cable Assembly

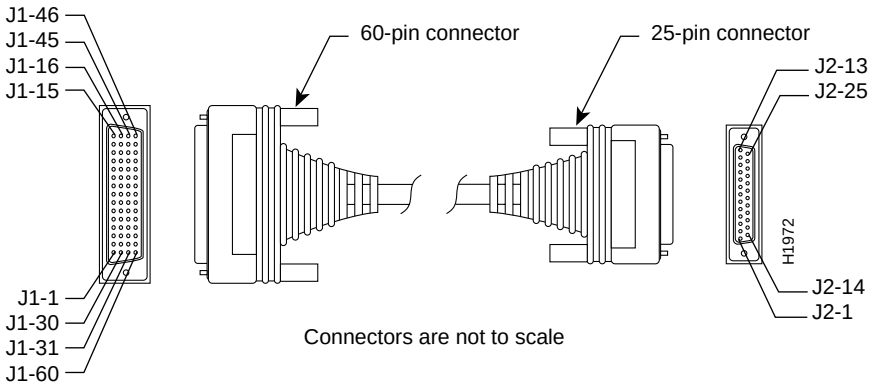


Table C-4 EIA/TIA-232 DTE Cable Pinout (DB-60 to DB-25)

60 Pin[1]	Signal	Description	Direction	25 Pin	Signal
J1-50	MODE_0	Shorting group	–	–	–
J1-51	GND				
J1-52	MODE_DCE				
J1-46	Shield GND	Single	–	J2-1	Shield GND
J1-41	TxD/RxD	Twisted pair no. 5	—>	J2-2	TxD
Shield	–		–	Shield	–
J1-36	RxD/TxD	Twisted pair no. 9	<—	J2-3	RxD
Shield	–		–	Shield	–
J1-42	RTS/CTS	Twisted pair no. 4	—>	J2-4	RTS
Shield	–		–	Shield	–
J1-35	CTS/RTS	Twisted pair no. 10	<—	J2-5	CTS
Shield	–		–	Shield	–
J1-34	DSR/DTR	Twisted pair no. 11	<—	J2-6	DSR
Shield	–		–	Shield	–
J1-45	Circuit GND	Twisted pair no. 1	–	J2-7	Circuit GND
Shield	–		–	Shield	–

60 Pin[1]	Signal	Description	Direction	25 Pin	Signal
J1-33 Shield	DCD/LL –	Twisted pair no. 12	<— –	J2-8 Shield	DCD –
J1-37 Shield	TxC/NIL –	Twisted pair no. 8	<— –	J2-15 Shield	TxC –
J1-38 Shield	RxC/TxCE –	Twisted pair no. 7	<— –	J2-17 Shield	RxC –
J1-44 Shield	LL/DCD –	Twisted pair no. 2	—> –	J2-18 Shield	LTST –
J1-43 Shield	DTR/DSR –	Twisted pair no. 3	—> –	J2-20 Shield	DTR –
J1-39 Shield	TxCE/TxC –	Twisted pair no. 6	—> –	J2-24 Shield	TxCE –

1. Any pin not referenced is not connected.

Table C-5 EIA/TIA-232 DCE Cable Pinout (DB-60 to DB-25)

60 Pin[1]	Signal	Description	Direction	25 Pin	Signal
J1-50 J1-51	MODE_0 GND	Shorting group	–	–	–
J1-46	Shield GND	Single	–	J2-1	Shield GND
J1-36 Shield	RxD/TxD –	Twisted pair no. 9	<— –	J2-2 Shield	TxD –
J1-41 Shield	TxD/RxD –	Twisted pair no. 5	—> –	J2-3 Shield	RxD –
J1-35 Shield	CTS/RTS –	Twisted pair no. 10	<— –	J2-4 Shield	RTS –
J1-42 Shield	RTS/CTS –	Twisted pair no. 4	—> –	J2-5 Shield	CTS –
J1-43 Shield	DTR/DSR –	Twisted pair no. 3	—> –	J2-6 Shield	DSR –

60 Pin[1]	Signal	Description	Direction	25 Pin	Signal
J1-45	Circuit GND	Twisted pair no. 1	–	J2-7	Circuit GND
Shield	–		–	Shield	
J1-44	LL/DCD	Twisted pair no. 2	—>	J2-8	DCD
Shield	–		–	Shield	–
J1-39	TxCE/TxC	Twisted pair no. 7	—>	J2-15	TxC
Shield	–		–	Shield	–
J1-40	NIL/RxC	Twisted pair no. 6	—>	J2-17	RxC
Shield	–		–	Shield	–
J1-33	DCD/LL	Twisted pair no. 12	<—	J2-18	LTST
Shield	–		–	Shield	–
J1-34	DSR/DTR	Twisted pair no. 11	<—	J2-20	DTR
Shield	–		–	Shield	–
J1-38	RxC/TxCE	Twisted pair no. 8	<—	J2-24	TxCE
Shield	–		–	Shield	–

1. Any pin not referenced is not connected.

EIA/TIA-449

Figure C-3 shows the EIA/TIA-449 cable assembly; Table C-6 lists the DTE pinout; Table C-7 lists the DCE pinout. Arrows indicate signal direction: —> indicates DTE to DCE, and <— indicates DCE to DTE.

Figure C-3 EIA/TIA-449 Cable Assembly

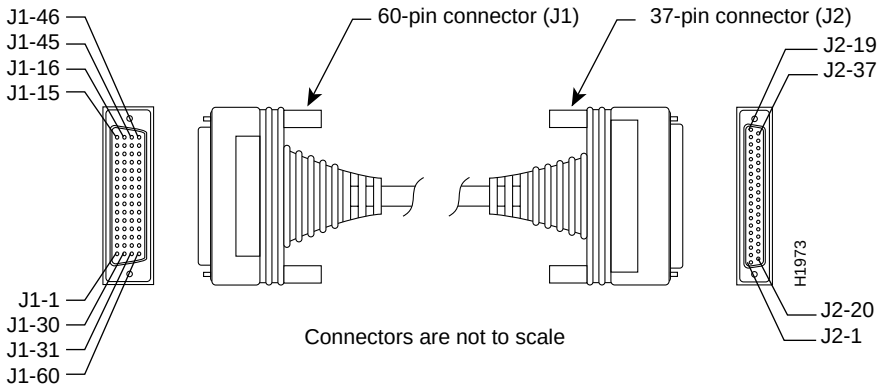


Table C-6 EIA/TIA-449 DTE Cable Pinout (DB-60 to DB-37)

60 Pin[1]	Signal	Description	Direction	37 Pin	Signal
J1-49 J1-48	MODE_1 GND	Shorting group	–	–	–
J1-51 J1-52	GND MODE_DCE	Shorting group	–	–	–
J1-46	Shield_GND	Single	_	J2-1	Shield GND
J1-11 J1-12	TxD/RxD+ TxD/RxD–	Twisted pair no. 6	—> —>	J2-4 J2-22	SD+ SD–
J1-24 J1-23	TxC/RxC+ TxC/RxC–	Twisted pair no. 9	<— <—	J2-5 J2-23	ST+ ST–
J1-28 J1-27	RxD/TxD+ RxD/TxD–	Twisted pair no. 11	<— <—	J2-6 J2-24	RD+ RD–
J1-9 J1-10	RTS/CTS+ RTS/CTS–	Twisted pair no. 5	—> —>	J2-7 J2-25	RS+ RS–
J1-26 J1-25	RxC/TxCE+ RxC/TxCE–	Twisted pair no. 10	<— <—	J2-8 J2-26	RT+ RT–

60 Pin[1]	Signal	Description	Direction	37 Pin	Signal
J1-1	CTS/RTS+	Twisted pair no. 1	<—	J2-9	CS+
J1-2	CTS/RTS–		<—	J2-27	CS–
J1-44	LL/DCD	Twisted pair no. 12	—>	J2-10	LL
J1-45	Circuit_GND		_	J2-37	SC
J1-3	DSR/DTR+	Twisted pair no. 2	<—	J2-11	DM+
J1-4	DSR/DTR–		<—	J2-29	DM–
J1-7	DTR/DSR+	Twisted pair no. 4	—>	J2-12	TR+
J1-8	DTR/DSR–		—>	J2-30	TR–
J1-5	DCD/DCD+	Twisted pair no. 3	<—	J2-13	RR+
J1-6	DCD/DCD–		<—	J2-31	RR–
J1-13	TxCE/TxC+	Twisted pair no. 7	—>	J2-17	TT+
J1-14	TxCE/TxC–		—>	J2-35	TT–
J1-15	Circuit_GND	Twisted pair no. 9	–	J2-19	SG
J1-16	Circuit_GND		–	J2-20	RC

1. Any pin not referenced is not connected.

Table C-7 EIA/TIA-449 DCE Cable Pinout (DB-60 to DB-37)

60 Pin[1]	Signal	Description	Direction	37 Pin	Signal
J1-49	MODE_1	Shorting group	–	–	–
J1-48	GND				
J1-46	Shield_GND	Single	–	J2-1	Shield GND
J1-28	RxD/TxD+	Twisted pair no. 11	<—	J2-4	SD+
J1-27	RxD/TxD–		<—	J2-22	SD–
J1-13	TxCE/TxC+	Twisted pair no. 7	—>	J2-5	ST+
J1-14	TxCE/TxC–		—>	J2-23	ST–
J1-11	TxD/RxD+	Twisted pair no. 6	—>	J2-6	RD+
J1-12	TxD/RxD–		—>	J2-24	RD–
J1-1	CTS/RTS+	Twisted pair no. 1	<—	J2-7	RS+
J1-2	CTS/RTS–		<—	J2-25	RS–

60 Pin[1]	Signal	Description	Direction	37 Pin	Signal
J1-24	TxC/RxC+	Twisted pair no. 9	—>	J2-8	RT+
J1-23	TxC/RxC–		—>	J2-26	RT–
J1-9	RTS/CTS+	Twisted pair no. 5	—>	J2-9	CS+
J1-10	RTS/CTS–		—>	J2-27	CS–
J1-29	NIL/LL	Twisted pair no. 12	—>	J2-10	LL
J1-30	Circuit_GND		–	J2-37	SC
J1-7	DTR/DSR+	Twisted pair no. 4	—>	J2-11	DM+
J1-8	DTR/DSR–		—>	J2-29	DM–
J1-3	DSR/DTR+	Twisted pair no. 2	<—	J2-12	TR+
J1-4	DSR/DTR–		<—	J2-30	TR–
J1-5	DCD/DCD+	Twisted pair no. 3	—>	J2-13	RR+
J1-6	DCD/DCD–		—>	J2-31	RR–
J1-26	RxC/TxCE+	Twisted pair no. 10	<—	J2-17	TT+
J1-25	RxC/TxCE–		<—	J2-35	TT–
J1-15	Circuit_GND	Twisted pair no. 8	_	J2-19	SG
J1-16	Circuit_GND		_	J2-20	RC

1. Any pin not referenced is not connected.

V.35

Figure C-4 shows the V.35 cable assembly; Table C-8 lists the DTE pinout; Table C-9 lists the DCE pinout. Arrows indicate signal direction: —> indicates DTE to DCE, and <— indicates DCE to DTE.

Figure C-4 V.35 Cable Assembly

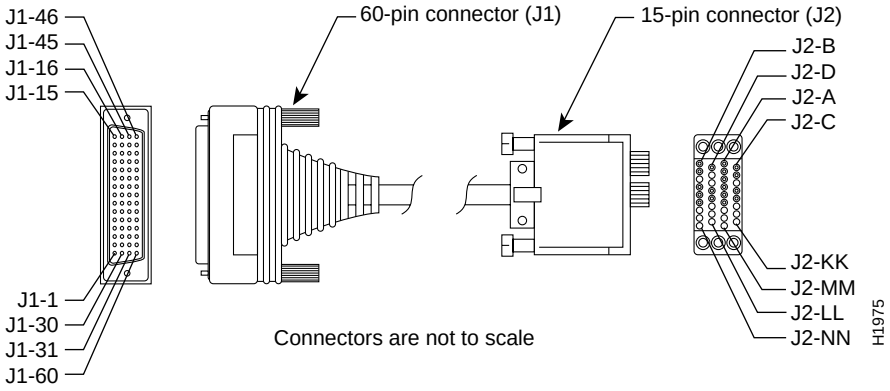


Table C-8 V.35 DTE Cable Pinout (DB-60 to 34-Pin)

60 Pin[1]	Signal	Description	Direction	34 Pin	Signal
J1-49 J1-48	MODE_1 GND	Shorting group	–	–	–
J1-50 J1-51 J1-52	MODE_0 GND MODE_DCE	Shorting group	–	–	–
J1-53 J1-54 J1-55 J1-56	TxC/NIL RxC_TxCE RxD/TxD GND	Shorting group	–	–	–
J1-46	Shield_GND	Single	–	J2-A	Frame GND

60 Pin[1]	Signal	Description	Direction	34 Pin	Signal
J1-45	Circuit_GND	Twisted pair no. 12	–	J2-B	Circuit GND
Shield	–		–	Shield	–
J1-42	RTS/CTS	Twisted pair no. 9	—>	J2-C	RTS
Shield	–		–	Shield	–
J1-35	CTS/RTS	Twisted pair no. 8	<—	J2-D	CTS
Shield	–		–	Shield	–
J1-34	DSR/DTR	Twisted pair no. 7	<—	J2-E	DSR
Shield	–		–	Shield	–
J1-33	DCD/LL	Twisted pair no. 6	<—	J2-F	RLSD
Shield	–		–	Shield	–
J1-43	DTR/DSR	Twisted pair no. 10	—>	J2-H	DTR
Shield	–		–	Shield	–
J1-44	LL/DCD	Twisted pair no. 11	—>	J2-K	LT
Shield	–		–	Shield	–
J1-18	TxD/RxD+	Twisted pair no. 1	—>	J2-P	SD+
J1-17	TxD/RxD–		—>	J2-S	SD–
J1-28	RxD/TxD+	Twisted pair no. 5	<—	J2-R	RD+
J1-27	RxD/TxD–		<—	J2-T	RD–
J1-20	TxCE/TxC+	Twisted pair no. 2	—>	J2-U	SCTE+
J1-19	TxCE/TxC–		—>	J2-W	SCTE–
J1-26	RxC/TxCE+	Twisted pair no. 4	<—	J2-V	SCR+
J1-25	RxC/TxCE–		<—	J2-X	SCR–
J1-24	TxC/RxC+	Twisted pair no. 3	<—	J2-Y	SCT+
J1-23	TxC/RxC–		<—	J2-AA	SCT–

1. Any pin not referenced is not connected.

Table C-9 V.35 DCE Cable Pinout (DB-60 to 34-Pin)

60 Pin[1]	Signal	Description	Direction	34 Pin	Signal
J1-49 J1-48	MODE_1 GND	Shorting group	–	–	–
J1-50 J1-51	MODE_0 GND	Shorting group	–	–	–
J1-53 J1-54 J1-55 J1-56	TxC/NIL RxC_TxCE RxD/TxD GND	Shorting group	–	–	–
J1-46	Shield_GND	Single	–	J2-A	Frame GND
J1-45 Shield	Circuit_GND –	Twisted pair no. 12	– –	J2-B Shield	Circuit GND –
J1-35 Shield	CTS/RTS –	Twisted pair no. 8	<— –	J2-C Shield	RTS –
J1-42 Shield	RTS/CTS –	Twisted pair no. 9	—> –	J2-D Shield	CTS –
J1-43 Shield	DTR/DSR –	Twisted pair no. 10	—> –	J2-E Shield	DSR –
J1-44 Shield	LL/DCD –	Twisted pair no. 11	—> –	J2-F Shield	RLSD –
J1-34 Shield	DSR/DTR –	Twisted pair no. 7	<— –	J2-H Shield	DTR –
J1-33 Shield	DCD/LL –	Twisted pair no. 6	<— –	J2-K Shield	LT –
J1-28 J1-27	RxD/TxD+ RxD/TxD–	Twisted pair no. 5	<— <—	J2-P J2-S	SD+ SD–
J1-18 J1-17	TxD/RxD+ TxD/RxD–	Twisted pair no. 1	—> —>	J2-R J2-T	RD+ RD–
J1-26 J1-25	RxC/TxCE+ RxC/TxCE–	Twisted pair no. 4	<— <—	J2-U J2-W	SCTE+ SCTE–
J1-22 J1-21	NIL/RxC+ NIL/RxC–	Twisted pair no. 3	—> —>	J2-V J2-X	SCR+ SCR–

60 Pin[1]	Signal	Description	Direction	34 Pin	Signal
J1-20	TxCE/TxC+	Twisted pair no. 2	—>	J2-Y	SCT+
J1-19	TxCE/TxC–		—>	J2-AA	SCT–

1. Any pin not referenced is not connected.

X.21

Figure C-5 shows the X.21 cable assembly; Table C-10 lists the DTE pinout; Table C-11 lists the DCE pinout. Arrows indicate signal direction: —> indicates DTE to DCE, and <— indicates DCE to DTE.

Figure C-5 X.21 Cable Assembly

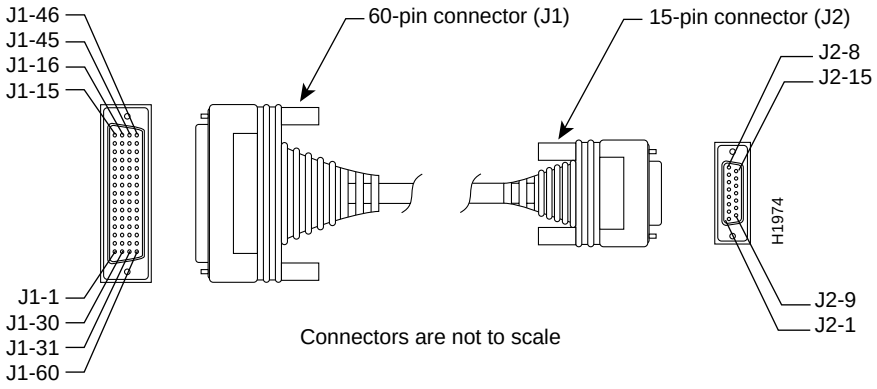


Table C-10 X.21 DTE Cable Pinout (DB-60 to DB-15)

60 Pin[1]	Signal	Description	Direction	15 Pin	Signal
J1-48 J1-47	GND MODE_2	Shorting group	–	–	–
J1-51 J1-52	GND MODE_DCE	Shorting group	–	–	–

60 Pin[1]	Signal	Description	Direction	15 Pin	Signal
J1-46	Shield_GND	Single	–	J2-1	Shield GND
J1-11	TxD/RxD+	Twisted pair no. 3	—>	J2-2	Transmit+
J1-12	TxD/RxD–		—>	J2-9	Transmit–
J1-9	RTS/CTS+	Twisted pair no. 2	—>	J2-3	Control+
J1-10	RTS/CTS–		—>	J2-10	Control–
J1-28	RxD/TxD+	Twisted pair no. 6	<—	J2-4	Receive+
J1-27	RxD/TxD–		<—	J2-11	Receive–
J1-1	CTS/RTS+	Twisted pair no. 1	<—	J2-5	Indication+
J1-2	CTS/RTS–		<—	J2-12	Indication–
J1-26	RxC/TxCE+	Twisted pair no. 5	<—	J2-6	Timing+
J1-25	RxC/TxCE–		<—	J2-13	Timing–
J1-15	Control_GND	Twisted pair no. 4	–	J2-8	Control GND
Shield	–		–	Shield	–

1. Any pin not referenced is not connected.

Table C-11 X.21 DCE Cable Pinout (DB-60 to DB-15)

60 Pin[1]	Signal	Description	Direction	15 Pin	Signal
J1-48	GND	Shorting group	–	–	–
J1-47	MODE_2				
J1-46	Shield_GND	Single	–	J2-1	Shield GND
J1-28	RxD/TxD+	Twisted pair no. 6	<—	J2-2	Transmit+
J1-27	RxD/TxD–		<—	J2-9	Transmit–
J1-1	CTS/RTS+	Twisted pair no. 1	<—	J2-3	Control+
J1-2	CTS/RTS–		<—	J2-10	Control–
J1-11	TxD/RxD+	Twisted pair no. 3	—>	J2-4	Receive+
J1-12	TxD/RxD–		—>	J2-11	Receive–
J1-9	RTS/CTS+	Twisted pair no. 2	—>	J2-5	Indication+
J1-10	RTS/CTS–		—>	J2-12	Indication–
J1-24	TxC/RxC+	Twisted pair no. 4	—>	J2-6	Timing+
J1-23	TxC/RxC–		—>	J2-13	Timing–

60 Pin[1]	Signal	Description	Direction	15 Pin	Signal
J1-15	Control_GND	Twisted pair no. 5	–	J2-8	Control GND
Shield	–		–	Shield	–

1. Any pin not referenced is not connected.

Ethernet Cable Assembly and Pinout

Figure C-6 shows an Ethernet (AUI) cable assembly, and Table C-12 lists an AUI cable pinout.

Figure C-6 Ethernet (AUI) Cable Assembly

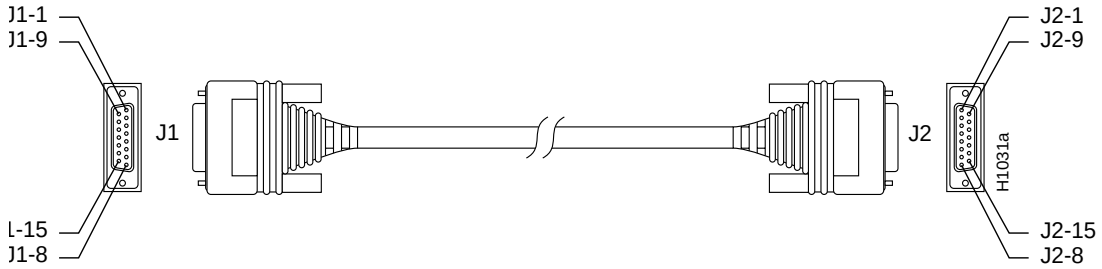


Table C-12 Ethernet (AUI) Cable Pinout (DB-15)

Pin[1]	Ethernet Circuit	Signal
3	DO-A	Data Out Circuit A
10	DO-B	Data Out Circuit B
11	DO-S	Data Out Circuit Shield
5	DI-A	Data In Circuit A
12	DI-B	Data In Circuit B
4	DI-S	Data In Circuit Shield

Pin[1]	Ethernet Circuit	Signal
2	CI-A	Control In Circuit A
9	CI-B	Control In Circuit B
1	CI-S	Control In Circuit Shield
6	VC	Voltage Common
13	VP	Voltage Plus
14	VS	Voltage Shield (L25 and M25)
Shell	PG	Protective Ground

1. Any pin not referenced is not connected.

Token Ring Pinout

Table C-13 lists the pinout for the Token Ring interface port.

Table C-13 Token Ring Port Pinout (DB-9)

9 Pin[1]	Signal
1	Receive
3	+5V[2]
5	Transmit
6	Receive
9	Transmit

1. Pins 2, 4, 7, and 8 are ground.
2. 600 mA maximum.

Asynchronous Serial Ports

Figure C-7 shows the RJ-45 breakout cable with pinouts for the 68-pin SCSI port and the RJ-45 serial port. Table C-14 contains the pinout for the RJ-45 end, and Table C-15 contains the pinout for the 68-pin SCSI type connector.

Figure C-7 Asynchronous Serial Interface Breakout Cable Assembly

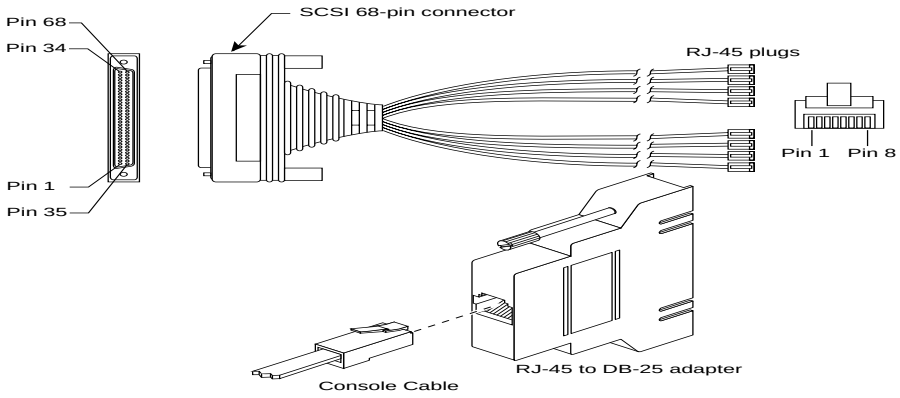


Table C-14 Asynchronous Breakout Cable Pinout (8-Pin RJ-45)

8-Pin RJ-45	Signal	Direction
1	CTS	<—
2	DSR/DCD	<—
3	RXD	<—
4	RXD/GND	—
5	TXD/GND	—
6	TXD	—>
7	DTR	—>
8	RTS	—>

Note The Asynchronous breakout cable is equivalent to a console or auxiliary port with a roll-over RJ-45 cable attached. See Table C-17 for asynchronous device connection options.

Table C-15 Asynchronous-Line Cable Pinout (68-Pin SCSI)

RJ-45 Plug	Pin	Signal	68-Pin SCSI (J1)
1	1	CTS	39
	2	DSR	5
	3	RXD	38
	4	RXD GND	4
	5	TXD GND	37
	6	TXD	3
	7	DTR	36
	8	RTS	2
2	1	CTS	43
	2	DSR	9
	3	RXD	42
	4	RXD GND	8
	5	TXD GND	41
	6	TXD	7
	7	DTR	40
	8	RTS	6

RJ-45 Plug	Pin	Signal	68-Pin SCSI (J1)
3	1	CTS	47
	2	DSR	13
	3	RXD	46
	4	RXD GND	12
	5	TXD GND	45
	6	TXD	11
	7	DTR	44
	8	RTS	10
4	1	CTS	51
	2	DSR	17
	3	RXD	50
	4	RXD GND	16
	5	TXD GND	49
	6	TXD	15
	7	DTR	48
	8	RTS	14
5	1	CTS	55
	2	DSR	21
	3	RXD	54
	4	RXD GND	20
	5	TXD GND	53
	6	TXD	19
	7	DTR	52
	8	RTS	18

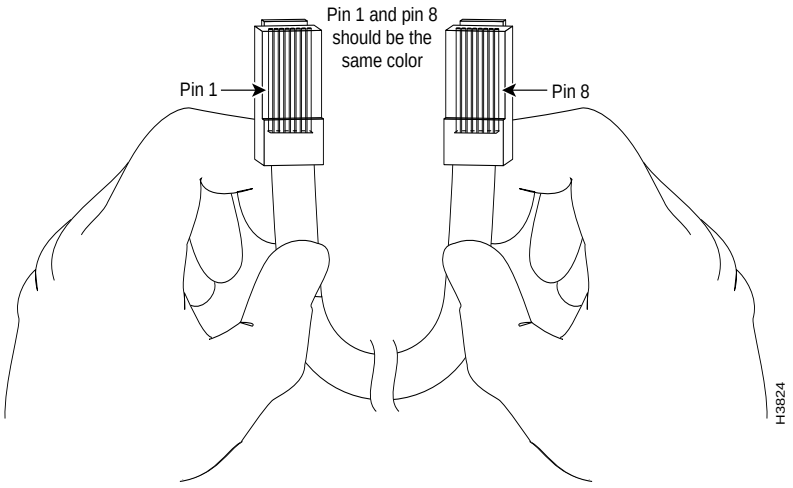
RJ-45 Plug	Pin	Signal	68-Pin SCSI (J1)
6	1	CTS	59
	2	DSR	25
	3	RXD	58
	4	RXD GND	24
	5	TXD GND	57
	6	TXD	23
	7	DTR	56
	8	RTS	22
7	1	CTS	53
	2	DSR	29
	3	RXD	62
	4	RXD GND	28
	5	TXD GND	61
	6	TXD	27
	7	DTR	60
	8	RTS	26
8	1	CTS	67
	2	DSR	33
	3	RXD	66
	4	RXD GND	32
	5	TXD GND	65
	6	TXD	31
	7	DTR	64
	8	RTS	30

RJ-45 Adapter Pinouts

Refer to Table C-16 for a list of the pins used on the RJ-45-to-DB-25 adapters, used with an RJ-45 cable, to connect terminals and modems to the Cisco 2500 series access server. The cable you use may be a roll-over cable or a straight cable.

A roll-over cable can be detected by comparing the two modular ends of the cable. Holding the cables in your hand, side-by-side, with the tab at the back, the wire connected to the pin on the outside of the left plug should be the same color as the pin on the outside of the right plug. If your cable was purchased from Cisco, pin 1 will be white on one connector, and pin 8 will be white on the other (a roll-over cable reverses pins 1 and 8, 2 and 7, 3 and 6, and 4 and 5). (See Figure C-8.)

Figure C-8 Identifying a Roll-Over Cable



The Cisco 2500 series access server ships with a rolled cable. Connection to a terminal or a modem will require an RJ-45-to-DB-25 adapter, and possibly a DB-25-to-DB9 adapter. Refer to Table C-17 for the cable and adapter configurations that can be used to connect terminals and modems to the Cisco 2500 series access server.

Table C-16 Pinouts for the RJ-45-to-DB-25 Adapters

Adapter	DTE M/F Pins[1]	DCE M/F Pins	MMOD Pins[2]
RJ-45 Pins	DB-25 Pins		
1	4	5	5
2	20	6	8
3	2	3	3
4	7	7	7
5	7	7	7
6	3	2	2
7	6	20	20
8	5	4	4

1. The female data terminal equipment (FDTE) adapter that is available from Cisco is labeled “Terminal.”
2. The MMOD adapter that is available from Cisco is labeled “Modem.”

Table C-17 Asynchronous Device Cabling Options

Access Server Port	RJ-45 Cable Type	DB-25 Adapter	End Device
Console or auxiliary	Rolled	FDTE[1]	Terminal
Console or auxiliary	Straight	FDCE	Terminal
Auxiliary or console	Rolled	MMOD[2]	Modem[3]

1. The FDTE RJ-45-to-DB-25 adapter is labeled “Terminal.”
2. The MMOD RJ-45-to-DB-25 adapter is labeled “Modem.”
3. The asynchronous breakout cable (see Table C-14 and Table C-15) is functionally equivalent to a roll-over cable.

APPENDIX D

Translated Safety Warnings

This appendix repeats in multiple languages the warnings in this publication.

Warning Definition

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.

Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

¡Atención! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

Jewelry Removal Warning

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Waarschuwing Alvorens aan apparatuur te werken die met elektrische leidingen is verbonden, sieraden (inclusief ringen, kettingen en horloges) verwijderen. Metalen voorwerpen worden warm wanneer ze met stroom en aarde zijn verbonden, en kunnen ernstige brandwonden veroorzaken of het metalen voorwerp aan de aansluitklemmen lassen.

Varoitus Ennen kuin työskentelet voimavirtajohtoihin kytkettyjen laitteiden parissa, ota pois kaikki korut (sormukset, kaulakorut ja kellot mukaan lukien). Metalliesineet kuumenevat, kun ne ovat yhteydessä sähkövirran ja maan kanssa, ja ne voivat aiheuttaa vakavia palovammoja tai hitsata metalliesineet kiinni liitäntänapoihin.

Attention Avant d'accéder à cet équipement connecté aux lignes électriques, ôter tout bijou (anneaux, colliers et montres compris). Lorsqu'ils sont branchés à l'alimentation et reliés à la terre, les objets métalliques chauffent, ce qui peut provoquer des blessures graves ou souder l'objet métallique aux bornes.

Warnung Vor der Arbeit an Geräten, die an das Netz angeschlossen sind, jeglichen Schmuck (einschließlich Ringe, Ketten und Uhren) abnehmen. Metallgegenstände erhitzen sich, wenn sie an das Netz und die Erde angeschlossen werden, und können schwere Verbrennungen verursachen oder an die Anschlußklemmen angeschweißt werden.

Avvertenza Prima di intervenire su apparecchiature collegate alle linee di alimentazione, togliersi qualsiasi monile (inclusi anelli, collane, braccialetti ed orologi). Gli oggetti metallici si riscaldano quando sono collegati tra punti di alimentazione e massa: possono causare ustioni gravi oppure il metallo può saldarsi ai terminali.

Advarsel Fjern alle smykker (inkludert ringer, halskjeder og klokker) før du skal arbeide på utstyr som er koblet til kraftledninger. Metallgjenstander som er koblet til kraftledninger og jord blir svært varme og kan forårsake alvorlige brannskader eller smelte fast til polene.

Aviso Antes de trabalhar em equipamento que esteja ligado a linhas de corrente, retire todas as jóias que estiver a usar (incluindo anéis, fios e relógios). Os objectos metálicos aquecerão em contacto com a corrente e em contacto com a ligação à terra, podendo causar queimaduras graves ou ficarem soldados aos terminais.

¡Advertencia! Antes de operar sobre equipos conectados a líneas de alimentación, quitarse las joyas (incluidos anillos, collares y relojes). Los objetos de metal se calientan cuando se conectan a la alimentación y a tierra, lo que puede ocasionar quemaduras graves o que los objetos metálicos queden soldados a los bornes.

Varning! Tag av alla smycken (inklusive ringar, halsband och armbandsur) innan du arbetar på utrustning som är kopplad till kraftledningar. Metallobjekt hettas upp när de kopplas ihop med ström och jord och kan förorsaka allvarliga brännskador; metallobjekt kan också sammansvetsas med kontakterna.

Installation Warning

Warning Read the installation instructions before you connect the system to its power source.

Waarschuwing Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.

Varoitus Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.

Attention Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.

Warnung Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.

Avvertenza Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.

Advarsel Les installasjonsinstruksjonene før systemet kobles til strømkilden.

Aviso Leia as instruções de instalação antes de ligar o sistema à sua fonte de energia.

¡Atención! Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.

Varning! Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.

TN Power Statement

Warning The device is designed to work with TN power systems.

Waarschuwing Het apparaat is ontworpen om te functioneren met TN energiesystemen.

Varoitus Koje on suunniteltu toimimaan TN-sähkövoimajärjestelmien yhteydessä.

Attention Ce dispositif a été conçu pour fonctionner avec des systèmes d'alimentation TN.

Warnung Das Gerät ist für die Verwendung mit TN-Stromsystemen ausgelegt.

Avvertenza Il dispositivo è stato progettato per l'uso con sistemi di alimentazione TN.

Advarsel Utstyret er utfomet til bruk med TN-strømsystemer.

Aviso O dispositivo foi criado para operar com sistemas de corrente TN.

¡Atención! El equipo está diseñado para trabajar con sistemas de alimentación tipo TN.

Varning! Enheten är konstruerad för användning tillsammans med elkraftssystem av TN-typ.

Circuit Breaker (15A) Warning

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

Waarschuwing Dit produkt is afhankelijk van de installatie van het gebouw voor kortsluit- (overstroom)beveiliging. Controleer of er een zekering of stroomverbreker van niet meer dan 120 Volt wisselstroom, 15 A voor de V.S. (240 Volt wisselstroom, 10 A internationaal) gebruikt wordt op de fasegeleiders (alle geleiders die stroom voeren).

Varoitus Tämä tuote on riippuvainen rakennukseen asennetusta oikosulkusuojauksesta (ylivirtasuojauksesta). Varmista, että vaihevirtajohtimissa (kaikissa virroitetuissa johtimissa) käytetään Yhdysvalloissa alle 120 voltin, 15 ampeerin ja monissa muissa maissa 240 voltin, 10 ampeerin sulaketta tai suojakytkintä.

Attention Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120 V alt., 15 A U.S. maximum (240 V alt., 10 A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

Warnung Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß- bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 240 V Wechselstrom, 10 A (bzw. in den USA 120 V Wechselstrom, 15 A) an den Phasenleitern (allen stromführenden Leitern) verwendet wird.

Avvertenza Questo prodotto dipende dall'installazione dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Verificare che un fusibile o interruttore automatico, non superiore a 120 VCA, 15 A U.S. (240 VCA, 10 A internazionale) sia stato usato nei fili di fase (tutti i conduttori portatori di corrente).

Advarsel Dette produktet er avhengig av bygningens installasjoner av kortslutningsbeskyttelse (overstrøm). Kontroller at det brukes en sikring eller strømbryter som ikke er større enn 120 VAC, 15 A (USA) (240 VAC, 10 A internasjonalt) på faselederne (alle strømførende ledere).

Aviso Este produto depende das instalações existentes para protecção contra curto-circuito (sobrecarga). Assegure-se de que um fusível ou disjuntor não superior a 240 VAC, 10A é utilizado nos condutores de fase (todos os condutores de transporte de corrente).

¡Atención! Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) deló propio edificio. Asegurarse de que se utiliza un fusible o interruptor automático de no más de 240 voltios en corriente alterna (VAC), 10 amperios del estándar internacional (120 VAC, 15 amperios del estándar USA) en los hilos de fase (todos aquéllos portadores de corriente).

Varning! Denna produkt är beroende av i byggnaden installerat kortslutningsskydd (överströmsskydd). Kontrollera att säkring eller överspänningsskydd används på fasledarna (samtliga strömförande ledare) ¥ för internationellt bruk max. 240 V växelström, 10 A (i USA max. 120V växelström, 15 A).

SELV Circuit Warning

Warning The ports labeled “Ethernet,” “10BaseT,” “Token Ring,” “Console,” and “AUX” are safety extra low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Because the BRI circuits are treated like telephone-network voltage, avoid connecting the SELV circuit to the telephone-network-voltage (TNV) circuits.

Waarschuwing De poorten die "Ethernet", "10BaseT", "Token Ring", "Console" en "AUX" zijn gelabeld, zijn veiligheidscircuits met extra lage spanning (genaamd SELV = Safety Extra Low Voltage). SELV circuits mogen alleen met andere SELV circuits verbonden worden. Omdat de BRI circuits op dezelfde manier als telefoonnetwerk-spanning behandeld worden, mag u het SELV circuit niet verbinden met de Telefoonnetwerk-spanning (TNV) circuits.

Varoitus Portit, joissa on nimet "Ethernet", "10BaseT", "Token Ring", "Console" ja "AUX", ovat erityisen pienen jännityksen omaavia turvallisuuspiirejä (SELV-piirejä). Tällaiset SELV-piirit tulee yhdistää ainoastaan muihin SELV-piireihin. Koska perusluokan liitäntöjen (Basic Rate Interface- eli BRI-liitännät) jännite vastaa puhelinverkoston jännitettä, vältä SELV-piirin yhdistämistä puhelinverkoston jännitepiireihin (TNV-piireihin).

Attention Les ports étiquetés « Ethernet », « 10BaseT », « Token Ring », « Console » et « AUX » sont des circuits de sécurité basse tension (Safety Extra Low Voltage ou SELV). Les circuits SELV ne doivent être interconnectés qu'avec d'autres circuits SELV. Comme les circuits BRI sont considérés comme des sources de tension de réseau téléphonique, éviter de connecter un circuit SELV à un circuit de tension de réseau téléphonique (telephone-network-voltage ou TNV).

Warnung Die mit "Ethernet", "10BaseT", "Token Ring", "Console" und "AUX" beschrifteten Buchsen sind Sicherheitsschaltungen mit extraniedriger Spannung (Safety Extra Low Voltage, SELV). SELV-Schaltungen sollten ausschließlich an andere SELV-Schaltungen angeschlossen werden. Da die BRI-Schaltungen wie Telefonnetzspannung behandelt werden, ist die SELV-Schaltung nicht an Telefonnetzspannungsschaltungen (TNV) anzuschließen.

Avvertenza Le porte contrassegnate da “Ethernet”, “10BaseT”, “TokenRing”, “Console” e “AUX” sono circuiti di sicurezza con tensione molto bassa (SELV). I circuiti SELV (Safety Extra Low Voltage - Tensione di sicurezza molto bassa) devono essere collegati solo ad altri circuiti SELV. Dato che i circuiti BRI vengono trattati come tensioni di rete telefonica, evitare di collegare il circuito SELV ai circuiti in cui è presente le tensione di rete telefonica (TNV).

Advarsel Utgangene merket "Ethernet", "10BaseT", "Token Ring", "Console" og "AUX" er lavspentkretser (SELV) for ekstra sikkerhet. SELV-kretser skal kun kobles til andre SELV-kretser. Fordi BRI-kretsene håndteres som telenettspenning, unngå å koble SELV-kretsen til kretser for telenettspenning (TNV).

Aviso As portas "Ethernet", "10BaseT", "Token Ring", "Console", and "AUX" são circuitos de segurança de baixa tensão (SELV). Estes circuitos deverão ser apenas ligados a outros circuitos SELV. Devido ao facto de os circuitos BRI (Interface de Ritmo Básico) serem tratados como sendo de tensão equivalente à da rede telefónica, evite ligar o circuito SELV aos circuitos TNV (tensão de rede telefónica).

¡Atención! Los puertos "Ethernet", "10BaseT", "Token Ring", "Console" y "AUX" son circuitos de baja señal (Safety Extra Low Voltage = SELV) que garantizan ausencia de peligro. Estos circuitos SELV deben ser conectados exclusivamente con otros también de tipo SELV. Puesto que los circuitos tipo BRI se comportan como aquéllos con voltajes de red telefónica, debe evitarse conectar circuitos SELV con circuitos de voltaje de red telefónica (TNV).

Varning! De portar som är märkta "Ethernet", "10BaseT", "Token Ring", "Console" och "AUX" är SELV-kretsar, d.v.s. skyddskretsar med extra låg spänning (SELV: Safety Extra-Low Voltage = skyddsklenspänning). SELV-kretsar får endast anslutas till andra SELV-kretsar. Eftersom BRI-kretsar behandlas liksom telefonnätsspänning bör SELV-kretsen inte anslutas till telefonnätsspänningskretsar (TNV-kretsar).

Power Supply Disconnection Warning

Warning Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

Waarschuwing Voordat u aan een frame werkt of in de nabijheid van voedingen, dient u bij wisselstroom toestellen de stekker van het netsnoer uit het stopcontact te halen en voor gelijkstroom toestellen dient u de stroom uit te schakelen bij de stroomverbreker.

Varoitus Kytke irti vaihtovirtalaitteiden virtajohto tai katkaise tasavirtalaitteiden virta suojakytkimellä, ennen kuin teet mitään asennuspohjalle tai työskentelet virtalähteiden läheisyydessä.

Attention Avant de travailler sur un châssis ou à proximité d'une alimentation électrique, débrancher le cordon d'alimentation des unités en courant alternatif ou couper l'alimentation des unités en courant continu au niveau du disjoncteur.

Warnung Bevor Sie an einem Chassis oder in der Nähe von Netzgeräten arbeiten, ziehen Sie bei Wechselstromeinheiten das Netzkabel ab bzw. schalten Sie bei Gleichstromeinheiten den Strom am Unterbrecher ab.

Avvertenza Prima di lavorare su un telaio o intorno ad alimentatori, scollegare il cavo di alimentazione sulle unità CA o scollegare l'alimentazione all’interruttore automatico sulle unità CC.

Advarsel Før det utføres arbeid på kabinettet eller det arbeides i nærheten av strømforsyningsenheter, skal strømledningen trekkes ut på vekselstrømsenheter, eller strømmen kobles fra ved strømbryteren på likestrømsenheter.

Aviso Antes de trabalhar num chassis, ou antes de trabalhar perto de unidades de fornecimento de energia, desligue o cabo de alimentação nas unidades de corrente alternada, ou desligue a corrente no disjuntor nas unidades de corrente contínua.

¡Atención! Antes de manipular el chasis de un equipo o trabajar cerca de una fuente de alimentación, desenchufar el cable de alimentación en los equipos de corriente alterna (CA), o cortar la alimentación desde el interruptor automático en los equipos de corriente continua (CC).

Varning! Innan du arbetar med ett chassi eller nära strömförsörjningsenheter skall du för växelströmsenheter dra ur nätsladden och för likströmsenheter bryta strömmen vid överspänningsskyddet.

Power Supply Warning

Warning Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.

Waarschuwing U dient de voeding niet aan te raken zolang het netsnoer aangesloten is. Bij systemen met een stroomschakelaar zijn er lijnspanningen aanwezig in de voeding, zelfs wanneer de stroomschakelaar uitgeschakeld is en het netsnoer aangesloten is. Bij systemen zonder een stroomschakelaar zijn er lijnspanningen aanwezig in de voeding wanneer het netsnoer aangesloten is.

Varoitus Älä kosketa virtalähdettä virtajohdon ollessa kytkettynä. Virrankatkaisimella varustetuissa järjestelmissä on virtalähteen sisällä jäljellä verkkojännite, vaikka virrankatkaisin on katkaistu-asennossa virtajohdon ollessa kytkettynä. Järjestelmissä, joissa ei ole virrankatkaisinta, on virtalähteen sisällä verkkojännite, kun virtajohto on kytkettynä.

Attention Ne pas toucher le bloc d'alimentation quand le cordon d'alimentation est branché. Avec les systèmes munis d'un commutateur marche-arrêt, des tensions de ligne sont présentes dans l'alimentation quand le cordon est branché, même si le commutateur est à l'arrêt. Avec les systèmes sans commutateur marche-arrêt, l'alimentation est sous tension quand le cordon d'alimentation est branché.

Warnung Berühren Sie das Netzgerät nicht, wenn das Netzkabel angeschlossen ist. Bei Systemen mit Netzschalter liegen Leitungsspannungen im Netzgerät vor, wenn das Netzkabel angeschlossen ist, auch wenn das System ausgeschaltet ist. Bei Systemen ohne Netzschalter liegen Leitungsspannungen im Netzgerät vor, wenn das Netzkabel angeschlossen ist.

Avvertenza Non toccare l'alimentatore se il cavo dell'alimentazione è collegato. Per i sistemi con un interruttore di alimentazione, tensioni di linea sono presenti all'interno dell'alimentatore anche quando l'interruttore di alimentazione è en posizione di disattivazione (off), se il cavo dell'alimentazione è collegato. Per i sistemi senza un interruttore, tensioni di linea sono presenti all'interno dell'alimentatore quando il cavo di alimentazione è collegato.

Advarsel Berør ikke strømforsyningsenheten når strømledningen er tilkoblet. I systemer som har en strømbryter, er det spenning i strømforsyningsenheten selv om strømbryteren er slått av og strømledningen er tilkoblet. Når det gjelder systemer uten en strømbryter, er det spenning i strømforsyningsenheten når strømledingen er tilkoblet.

Aviso Não toque na unidade abastecedora de energia quando o cabo de alimentação estiver ligado. Em sistemas com interruptor, a corrente eléctrica estará presente na unidade abastecedora, sempre que o cabo de alimentação de energia estiver ligado, mesmo quando o interruptor se encontrar desligado. Para sistemas sem interruptor, a tensão eléctrica dentro da unidade abastecedora só estará presente quando o cabo de alimentação estiver ligado.

¡Atención! No tocar la fuente de alimentación mientras el cable esté enchufado. En sistemas con interruptor de alimentación, hay voltajes de línea dentro de la fuente, incluso cuando el interruptor esté en Apagado (OFF) y el cable de alimentación enchufado. En sistemas sin interruptor de alimentación, hay voltajes de línea en la fuente cuando el cable está enchufado.

Varning! Vidrör inte strömförsörjningsenheten när nätsladden är ansluten. För system med strömbrytare finns det nätspänning i strömförsörjningsenheten även när strömmen har slagits av men nätsladden är ansluten. För system utan strömbrytare finns det nätspänning i strömförsörjningsenheten när nätsladden är ansluten.

Lightning Activity Warning

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity.

Waarschuwing Tijdens onweer dat gepaard gaat met bliksem, dient u niet aan het systeem te werken of kabels aan te sluiten of te ontkoppelen.

Varoitus Älä työskentele järjestelmän parissa äläkä yhdistä tai irrota kaapeleita ukkosilmalla.

Attention Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage.

Warnung Arbeiten Sie nicht am System und schließen Sie keine Kabel an bzw. trennen Sie keine ab, wenn es gewittert.

Avvertenza Non lavorare sul sistema o collegare oppure scollegare i cavi durante un temporale con fulmini.

Advarsel Utfør aldri arbeid på systemet, eller koble kabler til eller fra systemet når det tordner eller lyner.

Aviso Não trabalhe no sistema ou ligue e desligue cabos durante períodos de mau tempo (trovoada).

¡Advertencia! No operar el sistema ni conectar o desconectar cables durante el transcurso de descargas eléctricas en la atmósfera.

Varning! Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.